

# Integriteitszorg

## *Servicio di Impuesto, Aduana y Direccion (SIAD)*

Algemene Rekenkamer

2012

# Integriteitszorg

*Servicio di Impuesto,*

*Aduana y Direccion (SIAD)*

# Inhoud

# Resumen

Den e rapport aki, Algemene Rekenkamer ta presenta e resultadonan di su investigacion tocante e maneho di integridad na *Servicio di Impuesto, Aduana y Direccion* (SIAD). Cu e investigacion aki nos ta cumpli cu e peticion di Parlamento pa haci un investigacion di integridad na SIAD. E meta di e investigacion ta pa contribui na garantisa integridad y pa preveni falta di cumplimento cu normanan di integridad na SIAD. E pregunta central di nos investigacion tabata: den ki grado SIAD a implementa un maneho adecuado di integridad?

Nos descripcion di integridad pa e investigacion aki ta 'cumplimento cu normanan etico mara na e funcion'. E maneho di integridad ta e totalidad di medidanan pa stimula existencia di integridad den un organisacion. Den e investigacion nos a duna atencion specifico na siguridad di informacion. E proteccion di confidencia di informacion ta forma parti esencial di maneho di integridad.

E conclusion principal di nos investigacion ta cu e maneho di integridad na SIAD no ta adecuado. Esaki alabes ta e contesta riba nos pregunta central. Tin deficiencia den e structura y durabilidad di maneho di integridad y tin poco atencion pa stimula existencia di un cultura integro den e organisacion. Tambe nos ta constata cu e reglanan di integridad, e supervision riba cumplimento cu reglanan como tambe e forma di procede na momento cu wordo constata (posibel) infraccion di integridad, no ta completo.

Deficiencia den maneho di integridad ta significante pa un organisacion manera SIAD, cu ta eherce tareanan publico manera cobransa di impuesto y tarea di aduana. E tareanan aki tin un risico inherente di integridad halto. E interesnan (financiero) pa pagadonan di impuesto ta grandi y SIAD tin hopi informacion confidencial den su poder. Ademas di esaki, den e periodo di nos investigacion, SIAD tabata pasando den un proceso di reorganisacion y cambio. Esaki ta trece cune cu riesgonan di integridad ta bira ainda mas grandi, por ehempel pa motibo cu e lealtad/sinceridad di empleadonan por wordo presiona.

Den tabel 1 nos ta splica nos conclusion principal door di parti esaki den conclusionnan parcial.

**Tabel 1: Conclusionnan parcial**

| | |
|---|---|
| Structura y durabilidad di maneho di integridad | Tin deficiencia den e structura y durabilidad di maneho di integridad:<br>- No tin analisis structura di riesgonan di integridad of riesgo pa siguridad di informacion. Tampoco tin maneho documenta di integridad y siguridad di informacion. Medidanan cu ta wordo tuma hopi biaha ta basa riba incidentenan. Pesey esakinan por wordo categorisa como reactivo enbes di preventivo;<br>- No ta duna responsabilisacion riba ehecucion di maneho di integridad of siguridad di informacion. Un evaluacion di esakinan tampoco ta sosode.<br>SIAD no conoce un ciclo di maneho di integridad y siguridad di informacion. Pa e motibo aki e maneho no ta wordo realisa completamente y iniciativanan pa regla algo riba e tereno menciona no tin un efecto duradero. |
| Cultura | Tin poco atencion pa prevencion di infraccion di integridad y pa stimula un cultura integro den e organisacion:<br>- No tin codigo di conducta stipula y soft controls ta implementa den forma limita;<br>- Tin poco atencion pa e tema di integridad por ehempel durante combersacion di funcionamento of deliberacion relaciona cu trabou. Falta programanan pa conscientisa, haci training di dilema y investigacionnan tocante con e tema ta wordo experencia den e organisacion;<br>- Tin poco atencion pa e rol cu management ta carga pa duna e bon ehempel;<br>- Den practica tin falta di conscientisacion riba e echo cu maneho di integridad, bou cual tambe siguridad di informacion, ta primordialmente un responsabilidad di management di e organisacion. |
| Reglanan di integridad y supervision | - Te asina leu cu SIAD a desaroya maneho di integridad, e enfasis ta wordo poni riba reglanan cu e personal tin cu cumpli cu nan;<br>- Apesar di e atencion cu tin pa e reglanan di integridad, nos ta conclui cu ainda tin aspectonan cu mester wordo regla;<br>- E control y supervision riba cumplimento di reglanan di integridad no ta suficiente. SIAD no tin un funcionario of departamento encarga cu control interno. Ya pa varios aña caba CAD no a haci investigacion na Servicio di Impuesto. E rapport mas recien di CAD cu tabata concerni Aduana na 2010 ta indica deficiencianan riba tereno di maneho di integridad. CAD no a realisa control riba tereno di informacion automatisa tampoco. |
| Respons na momento di posibel infraccion di integridad | - No tin areglo interno pa trahadonan cu kier raporta (posibel) infraccion di integridad interno. Locual si ta existi ta un areglo (externo) di entregamento di keho. E problema cu e areglo aki ta, cu e confidencia/confiansa cu ta wordo priminti na esunnan cu ta entrega keho, no por wordo garantisa den tur circunstancia;<br>- No tin stipulacionnan concreto pa haci denuncia na momento cu tin (sospecho di) echonan castigabel, den caso cu e deber di haci denuncia, no ta stipula den ley.<br>- No tin un protocol di investigacion pa (posibel) infraccion di integridad of incidente cu ta concerni siguridad di informacion;<br>- Tin limitacion pa aplica medidanan di ordo pa motibo cu pa haci esaki ta rekeri un decision di minister. E decision pa impone castigo disciplinario, ta autoridad di minister y Gobernador. Den practica e procedura di castigonan disciplinario ta uno riguroso y lento. Pa e motibo aki e efectividad y credibilidad di castigonan disciplinario ta wordo cuestiona;<br>- Falta di registracion structura di casonan raporta, investigacion y castigo. Tampoco tin registracion di incidente riba tereno di siguridad di informacion. |

A base di e resultadonan di nos investigacion, nos ta recomenda e minister encarga cu Finansas pa (laga) desaroya e siguiente medidanan:

- Reforsa e cuadro y e ciclo di maneho di integridad como tambe siguridad di informacion na un manera structural:
  - Formula maneho di integridad y siguridad di informacion den cual metanan, puntonan di salida y medidanan ta incorpora. Laga esaki ta basa riba un ciclo di maneho completo (formula, ehecuta, evalua, y ahusta maneho);
  - Realisa analisis di riesgonan como base di maneho di integridad. Di e forma aki por señala y analisa riesgonan di integridad y siguridad. Incorpora e resultadonan di e analisisnan aki den (actualisacion di) maneho di integridad y siguridad di informacion;
  - Duna responsabilisacion riba e maneho por lo menos cada aña;
  - Laga haci evaluacion di e maneho periodicamente (por ehempel cada 3 pa 4 aña) pa asina ahusta esaki y pa duna e maneho un caracter duradero y structural.
- Pone enfasis riba e responsabilidad na prome luga di management, como tambe e ehempel cu management mester duna, pa loke ta trata maneho di integridad y siguridad di informacion. Evita cu e topiconan aki ta wordo considera principalmente e responsabilidad di departamento di Personal y Organisacion (P&O), respectivamente departamento di Informacion, Comunicacion y Tecnologia (ICT).
- Inverti den *soft controls*, por ehempel door di formula un codigo di conducta, apunta personanan di confiansa, organisa training (di dilema) y reunionnan informal, haci investigacionnan riba e forma con integridad ta wordo experencia den e organisacion, organisa actividadnan di conscientisacion tocante siguridad di informacion y mantene comunicacion directo riba temanan di integridad. Ta importante cu e inversionnan aki haya un caracter duradero. Un cultura integro y safe den un organisacion ta exigi mantencion continuo.
- Completa e reglanan y proceduranan di integridad existente pa asina kita e deficiencianan. Ta trata di reglanan y procedura cu ta preveni y combati e asina yama 'draaideurconstructies' (personanan cu ta sali for di servicio di gobierno y ta drenta bek riba termino cortico como consehero externo), intimidacion, discriminacion como tambe interesnan indesea (interesnan fuera di 'side jobs'). Por haci e areglo di aceptacion di regalo mas fuerte door di pone cu no ta acepta regalo di pagado di belasting, maske e balor financiero di e regalo ta insignificante. Tambe ta bon pa stipula un pakete coherente di regla y medida tocante siguridad di informacion como tambe pa e forma di trata informacion vulnerabel/confidencial.
- Introduci control/audits regular riba tereno di tanto integridad como siguridad di informacion. Aki ta trata di audits cu lo mester complementa e control interno den SIAD, audits (externo) di e responsabilisacion financiero como tambe e control di e maneho financiero y operacional den SIAD.
- Reforsa e instrumentonan cu ta uza pa por procede den caso di (posibel) infraccion di integridad:

- Formalisa un areglo/procedura interno cu ta regla e forma di raporta (sospecho di) infraccion di integridad of incidentenan relaciona cu siguridad. E procedura aki mester wordo comunica na tur trahado;
- Implementa un protocol pa por investiga caso di (posibel) infraccion di integridad y incidente relaciona cu siguridad di informacion;
- Fiha un procedura cla pa e forma di procede den caso di (sospecho di) echonan castigabel, na momento cu e obligacion pa haci denuncia no ta stipula pa ley;
- Percura pa un registracion structura di casonan cu a wordo raporta, incidentenan cu a tuma luga, investigacion cu a ser haci como tambe sancion cu a wordo duna.

Por ultimo nos ta recomenda e minister encarga cu Finansas pa autorisa direccion di SIAD pa medio di un mandato, pa bin cu medidanan disciplinario, en todo caso pa loke ta trata e castigonan mas leve (articulo 87, inciso 2 di Landsverordening Materieel Ambtenarenrecht (LMA)). Esaki lo stimula e posibel exito como tambe e credibilidad di medidanan disciplinario.

Dia 2 di november 2012 minister di Finansas a duna su reaccion riba nos rapport den concepto. Den su reaccion minister ta indica cu den e plan strategico di Servicio di Impuesto y Aduana, e lo duna atencion na stimula integridad di e organisacion. Minister lo uza nos rapport pa yuda implementa un maneho nobo di integridad y siguridad di informacion.
Minister ta duna algun remarca riba nos rapport. Den nos comentario final nos ta duna un splicacion tocante esaki.

Nos ta aprecia cu minister kier uza nos rapport pa formula un maneho nobo encuanto integridad y siguridad di informacion. Nos ta di opinion cu ainda minister no ta indica den cua forma y den ki termino e lo bay implementa nos sugerencianan. Nos ta sugeri minister pa informa Staten den un forma concreto con e ta bay implementa nos sugerencianan como tambe den ki termino e resultadonan di esaki lo ta visibel.

Nos lo aplaudi si nos rapport lo por tin un efecto mas grandi pa drecha e maneho di integridad na otro organisacionnan den gobierno, na unda ta existi deficiencianan similar. Algemene Rekenkamer semper ta dispuesto pa brinda e ayudo necesario den esaki.

# Samenvatting

In dit rapport doet de Algemene Rekenkamer verslag van het onderzoek naar de toereikendheid van het stelsel van integriteitszorg bij de *Servicio di Impuesto, Aduana y Direccion* (SIAD). Wij komen met dit onderzoek tegemoet aan het verzoek van de Staten om een integriteitsonderzoek bij de SIAD te verrichten. Het doel van dit onderzoek is om bij te dragen aan het waarborgen van de integriteit en het voorkomen van integriteitsinbreuken bij de SIAD. Onze probleemstelling was als volgt: in hoeverre heeft de SIAD een toereikend stelsel van integriteitszorg geïmplementeerd?

Voor dit onderzoek omschrijven wij integriteit als 'het naleven van aan de functie verbonden ethische normen'. Het stelsel van integriteitszorg is het geheel van maatregelen om integriteit binnen een organisatie te bevorderen. Wij hebben bij dit onderzoek specifiek aandacht besteed aan informatiebeveiliging, omdat de bescherming van de vertrouwelijkheid van informatie een belangrijk onderdeel is van integriteitszorg.

De hoofdconclusie van ons onderzoek, en tevens het antwoord op de probleemstelling, is dat het stelsel van integriteitszorg van de SIAD niet toereikend is. Zo zijn er gebreken in de structuur en duurzaamheid van de integriteitszorg en is er weinig aandacht voor het bevorderen van een integere cultuur. Verder zijn er lacunes in de integriteitsregels, in het toezicht op de naleving van integriteitsregels en in de response bij (mogelijke) integriteitsinbreuken.

Voor een organisatie als de SIAD zijn gebreken in de integriteitszorg van zwaarwegend belang, omdat de SIAD zich bezig houdt met publieke taken, zoals belastingheffing en douanetaken, die inherent een hoog integriteitsrisico hebben. Zo zijn de (financiële) belangen voor belastingplichtigen groot en is binnen de SIAD veel vertrouwelijke informatie aanwezig. Daarnaast verkeerde de SIAD ten tijde van het onderzoek in een reorganisatie- en veranderingsproces, waardoor integriteitsrisico's verhoogd worden, bijvoorbeeld omdat de loyaliteit van personeel onder druk kan komen te staan.

In tabel 1 werken we onze hoofdconclusie nader uit in deelconclusies.

**Tabel 1: Deelconclusies**

| | |
|---|---|
| Structuur en duurzaamheid van integriteitszorg | Er zijn gebreken in de structuur en duurzaamheid van het stelsel van integriteitszorg:<br>- Geen gestructureerde analyse van de integriteitsrisico's of van de risico's voor de informatiebeveiliging en ontbreken van een uitgeschreven integriteitsbeleid en informatiebeveiligingsbeleid. Voor zover maatregelen zijn getroffen, is dit vaak naar aanleiding van incidenten en daardoor reactief van karakter;<br>- Geen sprake van verantwoording over de uitvoering van integriteits- en informatiebeveiligingsbeleid of van een evaluatie daarvan.<br>De SIAD kent op het gebied van integriteitszorg en informatiebeveiliging geen beleidscyclus. Hierdoor komt beleid onvoldoende van de grond en verwateren eventuele initiatieven weer gemakkelijk en hebben deze daardoor geen duurzaam effect. |
| Cultuur | Weinig aandacht voor preventie van integriteitsinbreuken en voor het bevorderen van een integere cultuur:<br>- Geen vastgestelde gedragscode en slechts in beperkte mate *soft controls* geïmplementeerd;<br>- Weinig aandacht voor het onderwerp integriteit tijdens functioneringsgesprekken of werkoverleg en ontbreken van bewustwordingsprogramma's, dilemmatrainingen en belevingsonderzoek;<br>- Te weinig aandacht voor de voorbeeldrol van het management;<br>- In de praktijk blijft onderbelicht dat integriteitszorg, waaronder de informatiebeveiliging, vooral een managementverantwoordelijkheid is. |
| Integriteitsregels en toezicht | - Voor zover de SIAD het stelsel van integriteitszorg heeft ingevuld, ligt de nadruk vooral op het vaststellen van regels, waaraan het personeel zich heeft te houden;<br>- Ondanks de aandacht voor integriteitsregels, concluderen we dat er op onderdelen lacunes bestaan;<br>- Controle en toezicht op de naleving van integriteitsregels zijn onvoldoende. De SIAD beschikt niet over een interne controlefunctionaris of –afdeling. De CAD heeft al jaren geen onderzoek meer uitgevoerd bij het Belastingkantoor. Het meest recente CAD-rapport over de Douane uit 2010 wijst op tekortkomingen op het gebied van de integriteitszorg. Ook heeft de CAD geen IT audits[1] verricht. |
| Response bij mogelijke integriteits-inbreuken | - Geen meldingsregeling voor medewerkers die een (mogelijke) integriteitsinbreuk intern willen melden. Er is wel een (externe) klachtenregeling, maar de geheimhouding die in een folder over de klachtenregeling wordt beloofd aan de melders, is niet onder alle omstandigheden waar te maken;<br>- Geen heldere richtlijnen voor het doen van aangifte bij (verdenking van) strafbare feiten, in die gevallen dat er geen wettelijke aangifteplicht is;<br>- Geen protocol voor het onderzoek naar (mogelijke) integriteitsinbreuken of informatiebeveiligingsincidenten;<br>- Beperkte slagvaardigheid bij het treffen van ordemaatregelen, omdat daarvoor een beslissing van de minister nodig is. Beslissing over het opleggen van een disciplinaire straf is voorbehouden aan de minister en de Gouverneur. In de praktijk is de procedure van disciplinaire bestraffing omslachtig en traag, waardoor de effectiviteit en geloofwaardigheid van disciplinaire straffen onder druk komt te staan;<br>- Ontbreken van een gestructureerde registratie van meldingen, onderzoeken en bestraffingen. Ook geen registratie van incidenten op het terrein van informatiebeveiliging. |

[1] Onderzoek naar de toepassing van IT (informatietechnologie).

Op grond van de resultaten van ons onderzoek, bevelen we de minister belast met Financiën aan om de volgende maatregelen uit te (laten) werken:

- Versterk het beleidskader en de beleidscyclus voor de integriteitszorg en informatiebeveiliging structureel:
  - Formuleer een integriteitsbeleid en informatiebeveiligingsbeleid, waarin doelen, uitgangspunten en maatregelen zijn vastgelegd en dat uitgaat van een complete beleidscyclus (formuleren, uitvoeren, evalueren en bijstellen van beleid);
  - Voer ter onderbouwing van het beleid periodieke risicoanalyses uit om integriteits- en beveiligingsrisico's te signaleren en te analyseren. Verwerk de resultaten van deze analyses in (de actualisering van) het integriteits- en informatiebeveiligingsbeleid;
  - Leg ten minste jaarlijks verantwoording af over de uitvoering van het beleid. De SIAD dient verantwoording af te leggen aan de minister en de minister dient op zijn beurt verantwoording af te leggen aan het Parlement;
  - Laat het beleid periodiek (bijvoorbeeld eens in de drie of vier jaar) evalueren om het beleid bij te sturen en om het beleid een duurzaam en structureel karakter te geven.
- Benadruk de primaire verantwoordelijkheid en de voorbeeldrol van management voor integriteitszorg en informatiebeveiliging en voorkom dat deze onderwerpen vooral als een verantwoordelijkheid van de afdelingen Personeel en Organisatie (P&O), respectievelijk Informatie- en Communicatietechnologie (ICT) worden beschouwd.
- Investeer in *soft controls*, zoals het formuleren van een gedragscode, het aanstellen van vertrouwenspersonen, het verzorgen van (dilemma)trainingen en bijeenkomsten, het verrichten van belevingsonderzoek, het uitvoeren van bewustwordingsactiviteiten voor informatiebeveiliging en gerichte communicatie over integriteitsonderwerpen. Het is van belang dat deze investeringen een duurzaam en niet een eenmalig karakter hebben, omdat een integere en veilige cultuur in een organisatie voortdurend onderhoud vergt.
- Vul de bestaande integriteitsregels en –procedures aan om lacunes weg te nemen. Daarbij gaat het om regelingen ter voorkoming en bestrijding van 'draaideurconstructies', intimidatie, discriminatie en ongewenste nevenbelangen (anders dan nevenarbeid). De geschenkenregeling is aan te scherpen door niet toe te laten dat geschenken, ook wanneer ze een geringe financiële waarde hebben, worden geaccepteerd van belastingplichtigen. Stel ook een samenhangend pakket van regels en maatregelen vast voor de informatiebeveiliging en voor de omgang met gevoelige dossiers.
- Introduceer periodieke audits op het terrein van integriteit en informatiebeveiliging. Dit zijn specifieke gerichte audits die aanvullend zouden moeten zijn op de interne controle binnen de SIAD en op (externe) audits van de financiële verantwoordingen en van het financiële en operationele beheer bij de SIAD.
- Versterk de instrumenten voor de response bij (mogelijke) integriteitsinbreuken:

- Formaliseer een interne regeling voor het melden van (verdenkingen van) integriteitsinbreuken of beveiligingsincidenten en informeer alle medewerkers hierover;
- Stel een protocol vast voor onderzoek naar (mogelijke) integriteitsinbreuken en informatiebeveiligingsincidenten;
- Stel een heldere richtlijn vast voor het doen van aangifte bij (verdenking van) strafbare feiten, in die gevallen dat er geen wettelijke aangifteplicht is;
- Zorg voor een gestructureerde registratie van meldingen, incidenten, onderzoeken en bestraffingen.

Tot slot bevelen we de minister van Financiën aan om het treffen van ordemaatregelen en het opleggen van disciplinaire maatregelen, in ieder geval de lichtere vormen van disciplinaire bestraffing [2], naar de hoogste ambtelijke leiding van de SIAD te mandateren. Dit ter bevordering van de slagvaardigheid en geloofwaardigheid van disciplinaire maatregelen.

Op 2 november 2012 heeft de minister van Financiën gereageerd op een concept van ons rapport. Hij geeft in zijn reactie aan dat hij in het strategisch beleidsplan voor de belastingdienst en het douanekantoor rekening zal houden met het bevorderen van de integriteit van de dienst. Hij zal daarbij ons rapport gebruiken als bijdrage bij de implementatie van nieuw beleid inzake integriteit en informatiebeveiliging.
De minister plaatst verder enkele kanttekeningen bij ons rapport, waarop wij in ons nawoord een nadere toelichting geven.

Wij waarderen het dat de minister ons rapport wil gebruiken voor nieuw beleid inzake integriteit en informatiebeveiliging, maar vinden dat de minister in het midden laat hoe en wanneer hij onze aanbevelingen gaat implementeren. Wij raden de minister aan de Staten concreet te laten weten hoe hij de aanbevelingen gaat implementeren en wanneer de resultaten zichtbaar zullen zijn.

Wij zouden het tot slot een goede zaak vinden als ons rapport ook een bredere impuls geeft aan de verbetering van de integriteitszorg bij andere onderdelen van de overheid, voor zover daar vergelijkbare lacunes zijn waar te nemen. De Algemene Rekenkamer is gaarne bereid om hier waar mogelijk een helpende hand te bieden.

[2] Zie artikel 87, lid 2 van de LMA.

# 1 Inleiding

## 1.1 Verzoek van de Staten

De Staten van Aruba (Staten) hebben de Algemene Rekenkamer bij brief van 3 april 2012 verzocht om een integriteitsonderzoek bij de SIAD te verrichten. De Algemene Rekenkamer heeft de Staten laten weten graag tegemoet te komen aan dit verzoek en heeft tevens aangegeven zich daarbij te laten ondersteunen door de Nederlandse Algemene Rekenkamer.

Directe aanleiding voor het verzoek van de Staten is dat er informatie van belastingplichtigen is uitgelekt. Het onderzoek van de Algemene Rekenkamer is gericht op de maatregelen die de SIAD heeft getroffen om de integriteit van de organisatie te waarborgen. Het onderzoek betreft nadrukkelijk geen persoonsgericht onderzoek naar aanleiding van (verdenkingen van) integriteitsinbreuken.

## 1.2 Onderzoekskader

Het *doel* van het onderzoek is om bij te dragen aan het waarborgen van de integriteit en het voorkomen van integriteitsinbreuken bij de SIAD.
Daarom is de volgende *probleemstelling* gekozen: in hoeverre heeft de SIAD een toereikend stelsel van integriteitszorg geïmplementeerd?

*Stelsel van integriteitszorg*
Een centraal begrip in dit onderzoek is het stelsel van integriteitszorg. Daarom geven we in deze paragraaf een toelichting op dit begrip.
Voor dit onderzoek omschrijven we integriteit als ‘het naleven van aan de functie verbonden ethische normen’. Het aangrijpingspunt voor dit onderzoek is vooral de institutionele integriteit van de SIAD. Dit betekent dat de dienst zelf onkreukbaar en betrouwbaar dient te zijn. De integriteit van de organisatie dient ondersteund te worden door de integriteit van functionarissen die werkzaam zijn bij die organisatie. Tegenover de verantwoordelijkheid van individuele medewerkers staat de verantwoordelijkheid van de leidinggevenden van de SIAD om verleidingen weg te

nemen en beheersmaatregelen te treffen om integriteitsinbreuken te voorkomen en om in te kunnen grijpen bij incidenten.

Het stelsel van integriteitszorg is het geheel van maatregelen om integriteit binnen een organisatie te bevorderen. Dit stelsel omvat in hoofdlijnen de volgende elementen:

- Beleidskader integriteit.
  Om de integriteit van een organisatie te kunnen waarborgen, zal het management een gestructureerd kader van beheersingsmaatregelen dienen in te richten. Dat betekent onder andere dat het management inzicht dient te hebben in de integriteitsrisico's en op basis daarvan een integriteitsbeleid dient te formuleren. Dit beleid wordt geconcretiseerd in een gedragscode, waarin op hoofdlijnen kernwaarden en gedragsregels op het terrein van integriteit worden vastgelegd. Over het gevoerde integriteitsbeleid dient verantwoording te worden afgelegd en periodiek is een beleidsevaluatie nodig om te bezien of bijstellingen in het integriteitsbeleid nodig zijn.
- Integriteitsregels.
  Voor alle medewerkers zijn op het terrein van integriteit regels nodig, zodat helder is binnen welke kaders gewerkt dient te worden en welk gedrag (niet) acceptabel is. Deze integriteitsregels vormen een nadere uitwerking van de gedragscode.
- *Soft controls*.
  Onder *soft controls* worden beheersmaatregelen verstaan die gericht zijn op het bevorderen van een integere cultuur in een organisatie. Zo dienen waarden en normen regelmatig onder de aandacht van het personeel te worden gebracht, waardoor houding en gedrag van medewerkers positief worden beïnvloed. Managers en bestuurders hebben hierin een belangrijke voorbeeldfunctie te vervullen.
- Interne controle en accountantscontrole.
  Interne controle en accountantscontrole zijn nodig om de naleving van het integriteitsbeleid te beoordelen. De onderzoeken van de interne controleur of accountant dienen te leiden tot conclusies en aanbevelingen en de organisatie dient lering te trekken uit de onderzoeksresultaten.
- Response bij mogelijke integriteitsinbreuken.
  Ook al treft een organisatie preventieve maatregelen om de integriteit van een organisatie te waarborgen, er zal rekening gehouden moeten worden met de mogelijkheid dat er signalen worden ontvangen van mogelijke inbreuken. De organisatie dient over procedures te beschikken om signalen en meldingen te ontvangen en te registreren. Vervolgens dient een organisatie te beschikken over procedures voor het onderzoek van signalen en meldingen. De organisatie dient een registratie bij te houden van de (uitkomsten van de) onderzoeken, de vastgestelde inbreuken en van de disciplinaire straffen.

Voor een uitgebreide beschrijving van het normenkader voor integriteitszorg verwijzen we naar de methodologische verantwoording, die als bijlage bij dit rapport is gevoegd.

*Informatiebeveiliging*
Gelet op de aanleiding van dit onderzoek hebben wij, waar relevant, specifiek aandacht besteed aan informatiebeveiliging, omdat de bescherming van de vertrouwelijkheid van informatie een belangrijk onderdeel is van integriteitszorg. Informatiebeveiliging definiëren we als het geheel van maatregelen om de beschikbaarheid, betrouwbaarheid en vertrouwelijkheid van informatie te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel niveau te beperken.

## 1.3 Organisatie SIAD

De *Servicio di Impuesto, Aduana y Direccion* (SIAD) ressorteert onder de minister belast met Financiën. De SIAD bestaat uit drie onderdelen, namelijk de *Direccion di Impuesto y Aduana* (Directie), de *Servicio di Impuesto* (Belastingdienst) en de *Servicio di Aduana* (Douane).
De Directie bestaat uit ongeveer 25 medewerkers en heeft verantwoordelijkheden op het terrein van fiscaal beleid en wetgeving, personeel, organisatie, communicatie en informatiesystemen van de SIAD.
De Belastingdienst bestaat uit ruim 200 medewerkers en voert het primaire belastingproces uit, namelijk het heffen, innen en controleren van belastinggelden.
De Douane bestaat ook uit ruim 200 medewerkers en voert het primaire invoerrechten- en accijnzenproces uit. De Douane heeft een toezichthoudende taak ten aanzien van het grensoverschrijdend goederenverkeer, bijvoorbeeld verdovende middelen, geneesmiddelen en beschermde diersoorten.
De minister van Financiën, Communicatie, Utiliteiten en Energie (minister van Financiën) heeft op 16 november 2010 een managementteam SIAD in het leven geroepen. Dit managementteam heeft onder andere de taak om verbeteringen in het functioneren van de SIAD door te voeren, zoals:

- het opstellen van een strategisch beleidsplan voor de SIAD;
- het inhalen van de achterstanden op het gebied van de directe en indirecte belastingen;
- de hervorming van de belastingen;
- het opzetten en beschrijven van de administratieve organisatie van de organisatie;
- het opleveren van periodieke managementinformatie.

Ten tijde van ons onderzoek werd er ook gewerkt aan de loskoppeling van de Douane van de SIAD. De streefdatum voor deze loskoppeling is 1 januari 2013.

## 1.4 Leeswijzer

Na dit inleidende hoofdstuk, presenteren we in de hoofdstukken 2 tot en met 6 onze bevindingen over het stelsel van integriteitszorg bij de SIAD. Achtereenvolgens gaan we in op het beleidskader voor integriteit (hoofdstuk 2), integriteitsregels (hoofdstuk 3), *soft controls* (hoofdstuk 4), interne en accountantscontrole (hoofdstuk 5) en op de response bij mogelijke integriteitsinbreuken (hoofdstuk 6).

Hoofdstuk 7 bevat de conclusies en aanbevelingen die wij baseren op de bevindingen over het stelsel van integriteitszorg. Tot slot is in hoofdstuk 8 de bestuurlijke reactie van de minister van Financiën weergegeven en ons nawoord.

# 2 Beleidskader integriteit

## 2.1 Risicoanalyse

Om een stevig fundament te leggen voor de integriteitsmaatregelen in een organisatie, is inzicht in integriteitsrisico's een vereiste. Dit inzicht kan worden verkregen door een risicoanalyse toe te passen, waaruit de kwetsbaarheden van de organisatie naar voren komen.
In de publieke sector behoren de Belastingdienst en de Douane, door de aard van de werkzaamheden, tot de inherent zeer kwetsbare overheidsdiensten. Zo spelen er grote financiële belangen voor de belastingplichtigen, is er omvangrijk betalingsverkeer en gaat het om zeer gevoelige en vertrouwelijke informatie. Het is dus van groot belang dat de kwetsbaarheden in kaart zijn gebracht.
Bij de analyse van integriteitsrisico's dienen ook kwetsbaarheidsverhogende omstandigheden in de beschouwing te worden betrokken. Dergelijke omstandigheden kunnen bijvoorbeeld aan de orde zijn als een overheidsorganisatie te maken heeft met complexe regelgeving en/of met ingrijpende veranderingsprocessen.

Uit ons onderzoek blijkt dat de SIAD geen gestructureerde analyse heeft verricht of laten verrichten naar de integriteitsrisico's bij de dienst als basis voor het integriteitsbeleid. Omdat geen risicoanalyse is uitgevoerd, heeft de SIAD ook de mogelijkheid onbenut gelaten om op deze wijze het management en de medewerkers bewust te maken van kwetsbaarheden op het terrein van integriteit.

Tot de integriteitsrisico's behoren ook risico's dat inbreuken plaatsvinden op de vertrouwelijkheid van informatie. Op dit punt geldt dat voor de informatiebeveiliging ook een stevig fundament dient te worden gelegd in de vorm van een gestructureerde risicoanalyse. In deze analyse dienen de risico's voor onder andere de vertrouwelijkheid van informatie te worden geïdentificeerd en dient ook het belang van de risico's te worden afgewogen. De resultaten van een risicoanalyse geven richting aan het selecteren van maatregelen voor het beheersen van informatiebeveiligingsrisico's.

Op het terrein van informatiebeveiliging heeft SIAD geen gestructureerde risicoanalyse verricht of laten verrichten waarmee de volledige organisatie en alle

informatie(systemen) worden afgedekt. In de aangetroffen conceptnotities van de IT-afdeling met verbeterplannen op het gebied van IT is er wel impliciet aandacht voor enkele specifieke kwetsbaarheden van IT, zoals de printomgeving, e-mail en harde schijven.

## 2.2 Integriteitsbeleid

Via het integriteitsbeleid maakt het management van een organisatie duidelijk welk belang het hecht aan integriteit en welke doelen het management op integriteitsgebied nastreeft. Het beleid moet ook duidelijk maken welke plannen voor de realisatie dienen te worden uitgevoerd en binnen welk tijdpad.

Bij de SIAD ontbreekt een uitgeschreven integriteitsbeleid. Daardoor ontbreekt op dit terrein een helder beleidskader dat door het management en de medewerkers wordt gedragen. Zoals blijkt uit de volgende hoofdstukken zijn er in het verleden op onderdelen wel maatregelen op het terrein van integriteit genomen, maar een verbindend kader ontbreekt. Daardoor zijn er lacunes en is de samenhang tussen de maatregelen beperkt. Maatregelen worden vaak naar aanleiding van incidenten genomen en zijn daardoor reactief van karakter.

Op het gebied van de informatiebeveiliging hebben we soortgelijke bevindingen als voor het integriteitsbeleid. Een informatiebeveiligingsbeleid is een essentieel instrument voor het management om richting te geven aan informatiebeveiliging in overeenstemming met de organisatiedoelstellingen. In het informatiebeveiligingsbeleid legt het management vast welke strategische doelen op het gebied van informatiebeveiliging worden nagestreefd en op welke wijze deze zullen worden gerealiseerd. Het beleid dient kenbaar te worden gemaakt aan het personeel. Bij de SIAD ontbreekt een dergelijk integraal en uitgeschreven beleid inzake informatiebeveiliging. Logisch uitvloeisel hiervan is dat het informatiebeveiligingsbeleid niet kenbaar is gemaakt aan het personeel.

## 2.3 Gedragscode

Een gedragscode geeft de kernwaarden van een organisatie aan, waarbij het van belang is dat zowel het management als de medewerkers deze waarden delen en levend houden. De gedragscode behoort normerend te zijn, in de zin dat er in hoofdlijnen ook regels dienen te zijn geformuleerd voor (on)aanvaardbaar gedrag met de daarbij behorende sancties. Daarbij dient te worden aangesloten op geldende wet- en regelgeving. De hoofdregels uit een gedragscode behoren nader uitgewerkt te worden in meer gedetailleerde integriteitsregels (zie hoofdstuk 3).

De SIAD heeft geen gedragscode voor het personeel vastgesteld, waarin de kernwaarden en de integriteitsregels van de organisatie op hoofdlijnen zijn beschreven.
In een nota van 9 februari 1999, *Kenmerken van een deugdelijke en effectieve Belastingadministratie* zijn wel kenmerken beschreven van een efficiënte, moderne en professionele belastingadministratie. In dit document is onder punt 1.1 aangegeven dat een strikte gedragscode vereist is voor de ethische en professionele uitoefening van de functie en voor het persoonlijk gedrag van de belastingambtenaar. De gedragscode zelf ontbreekt echter.
Op het intranet van de SIAD is een beschrijving van de visie en missie van de dienst te vinden. Als basiswaarden worden professionaliteit, respect en integriteit genoemd, maar dit is verder niet uitgewerkt.
Voor het SIAD-personeel bestaat er een *Werkwijzer*, die is bedoeld als een huishoudelijk reglement. Het document is niet geschreven op het niveau van een gedragscode, maar betreft vooral een samenvatting van meer gedetailleerde integriteits- en omgangsregels bij de SIAD (zie hoofdstuk 3).

## 2.4 Evaluatie en verantwoording

Evenals bij ander beleid is het voor integriteitsbeleid, en meer specifiek ook voor informatiebeveiligingsbeleid, van belang dat een volledige beleidscyclus wordt ingericht: beleid formuleren, uitvoeren, evalueren en bijstellen. Op die manier wordt bevorderd dat het beleid actueel en effectief is.

Omdat de SIAD geen integriteits- en informatiebeveiligingsbeleid heeft geformuleerd, is er ook geen sprake van een verantwoording over de uitvoering van dit beleid of van een evaluatie daarvan.
In het algemeen heeft de SIAD de afgelopen jaren geen externe verantwoording (jaarverslag) uitgebracht. Dit betekent dat er ook geen externe verantwoording is over het gevoerde integriteits- en informatiebeveiligingsbeleid.

# 3 Integriteitsregels

Integriteitsregels geven voorschriften of richtlijnen voor ambtenaren en hun gedragingen. De integriteitsregels geven aan waaraan een ambtenaar zich heeft te houden en welk gedrag (niet) acceptabel is. Integriteitsregels kunnen ook betrekking hebben op specifieke procedurele voorschriften die tot doel hebben de integriteit te bevorderen.

*Strafwettelijke regels*

De zwaarste integriteitsregels voor de overheid, waaronder de SIAD, zijn neergelegd in het Wetboek van Strafrecht van Aruba. Belangrijke bepalingen die in dit wetboek te vinden zijn betreffen:

- de schending van geheimen (Tweede boek; Titel XVII; artikel 285);
- de ambtsmisdrijven (Tweede boek; Titel XXVIII; artikelen 373-394);
- de ambtsovertredingen (Derde Boek; Titel VIII; artikelen 484–492a).

In dit wetboek zijn onder meer bepaalde vormen van fraude, corruptie, misbruik van gezag en belangenverstrengeling strafbaar gesteld.

*Landsverordening Materieel Ambtenarenrecht*

De SIAD valt verder onder de landsverordeningen die voor de gehele overheid gelden. Voor wat betreft het onderwerp integriteit is vooral de Landsverordening Materieel Ambtenarenrecht (LMA; AB 1989 no. GT 37 en latere wijzigingen) van belang.

De LMA bevat onder andere de volgende bepalingen, die zijn op te vatten als integriteitsregels:

- Verklaring omtrent goed zedelijk gedrag bij indiensttreding (artikel 6)[3];
- Periodieke verhogingen in relatie tot disciplinaire straffen (artikel 19);
- Eed of belofte (artikel 46);
- Plicht zich te gedragen zoals een goed ambtenaar betaamt (artikel 47);
- Ontzegging van toegang tot gebouwen of werk (artikel 48);
- Handhaving van werktijden (artikel 49, lid 1-3);
- Alcoholverbod (artikel 49, lid 4);
- Nevenarbeid (artikel 55);
- Belangenvermenging (artikel 56, 57 en 57a);

[3] Uit de interviews is naar voren gekomen dat voor bepaalde functies bij de SIAD, vooral bij de Douane, niet alleen een verklaring omtrent goed zedelijk gedrag vereist is, maar ook een screening door de Veiligheidsdienst Aruba (VDA).

- Gebruik van overheidsgoederen (artikel 58);
- Aannemen giften (artikel 59-61);
- Geheimhouding (artikel 62);
- Vergoeding kosten dienstreizen (artikel 73);
- Klachtenregeling (artikel 78);
- Disciplinaire straffen (artikel 82-86);
- Schorsing en ontslag (artikel 87).

In het handboek van de Directie Personeel en Organisatie (DPO[4]) van 27 juli 2007 zijn de integriteitsregels verder uitgewerkt en voorzien van procedurebeschrijvingen. Hoofdstuk 1 van dit handboek gaat in op de disciplinaire zaken en hoofdstuk 14 op de overige rechten en plichten, waarbij een belangrijk deel van de hiervoor genoemde integriteitsregels aan de orde komt.

*Integriteitsregels van SIAD*

In aanvulling op de integriteitsregels en –procedures van de DPO, respectievelijk de DRH, heeft de SIAD verschillende onderwerpen verder uitgewerkt in gedragsregels, aanschrijvingen, procedures, regelingen of dienstorders:

- Klachtenprocedure (2009);
- Aanschrijving nevenwerkzaamheden (ongedateerd);
- Geschenkenregeling Belastingdienst (1 december 2000);
- Procedure kleine kas (ongedateerd);
- Gedragsregel digitale voorzieningen (25 juni 2008);
- Gedragsregels gebruik interne en externe email SIAD (ongedateerd);
- Aangifteplicht artikel 200 Wetboek van Strafvordering (19 april 1999);
- Aanhouding ambtenaar (maart 2004);
- Protocol informatieverstrekking door OM[5] (12 september 2006);
- Dienstorder Douane: reizen naar Venezuela met pleziervaartuigen (19 april 2011);
- Dienstorder Douane: geld lenen bij klanten van de Douane (24 september 2010);
- Informatie disciplinaire en rechtspositionele maatregelen ten behoeve van Direccion di Impuesto y Aduana (juni 2004).

*Kanttekeningen bij de integriteitsregels*

De LMA en de verschillende aanvullingen van de SIAD omvatten de meest gangbare integriteitsregels. Toch ontbreken enkele onderdelen die ook van belang kunnen zijn voor de SIAD.

Bij de SIAD zijn er bijvoorbeeld geen regels die moeten voorkomen dat uit dienst tredend personeel direct of binnen een korte termijn weer wordt ingehuurd als

[4] inmiddels Departamento Recurso Humano (DRH)

[5] Openbaar Ministerie

extern adviseur (tegengaan van 'draaideurconstructies'). Ook zijn er geen integriteitsregels gesteld om intimidatie, discriminatie en andere ongewenste omgangsvormen op de werkplek tegen te gaan.

Bij de beschikbare regelingen kunnen de volgende kanttekeningen worden geplaatst:

- Er is een regeling voor nevenarbeid, maar daarmee zijn niet alle ongewenste nevenbelangen afgedekt. Er is geen bepaling die het ambtenaren verbiedt om (financiële) nevenbelangen, anders dan nevenarbeid, aan te gaan of aan te houden, die in strijd (kunnen) komen met een goede functievervulling. Artikel 57 LMA maakt het mogelijk om ambtenaren te verbieden commissaris, bestuurder, vennoot, aandeelhouder of lid te zijn van nader te noemen vennootschappen, stichtingen of verenigingen, maar dit vereist een specifiek verbodsbesluit van het bevoegd gezag. Bovendien kunnen ook andere financiële belangen, zoals bijvoorbeeld leningen, aan de orde zijn.
- De Belastingdienst hanteert een geschenkenregeling die een aanvulling vormt op artikel 59 LMA: "*Het is de ambtenaar verboden een gift of een belofte daartoe van een derde aan te nemen, waarvan hij weet of redelijkerwijze moet vermoeden, dat deze gedaan wordt teneinde hem te bewegen in zijn bediening iets te doen of na te laten*". De geschenkenregeling van de Belastingdienst onderkent dat de bepaling van artikel 59 LMA onduidelijk is, omdat het aannemen van een gift alleen verboden is als er een element van 'tegenprestatie' bij zou spelen. Dit is in de praktijk lastig vast te stellen en/of te bewijzen. De Belastingdienst heeft daarom aanvullende regels opgesteld die een waardegrens aangeven (maximaal Afl. 50) en kaders stellen voor de openheid en de soort giften. De geschenkenregeling van de SIAD impliceert dat een gift in de relatie tussen belastingplichtige en Belastingdienst niet onder alle omstandigheden wordt afgewezen.
- De gedragsregels digitale voorzieningen en gebruik interne en externe email bevatten voorschriften voor de medewerkers om misbruik van computervoorzieningen te voorkomen. Het management van de SIAD heeft echter geen samenhangend pakket van beveiligingsmaatregelen vastgesteld om inbreuken op de vertrouwelijkheid van de informatie te voorkomen. In de praktijk zijn er overigens wel maatregelen getroffen om de toegang tot gebouwen en informatie te beveiligen, maar de opzet mist een duidelijke structuur en de implementatie in de organisatie is gebrekkig. Zo is er een procedure beschreven voor het beheer van systeemautorisaties, maar deze bleek bij een deel van de relevante medewerkers onbekend en niet aan te sluiten op de gang van zaken in de praktijk. Verder heeft de waarnemend manager IT, naar aanleiding van beveiligingsincidenten, voorstellen gedaan om enkele specifieke informatiebeveiligingsmaatregelen te treffen. Ten tijde van de uitvoering van ons onderzoek, moest het management van de SIAD daar nog

een beslissing over nemen. Het betreft voorstellen voor de printersituatie (concept, mei 2012), data en informatiebeveiliging (concept, 8 juni 2012) en huisregels, veiligheidsregels en toegangsregels ten behoeve van de medewerkers van de IT-afdeling (concept, mei 2012). Uit de interviews in het kader van ons onderzoek is naar voren gekomen dat externe medewerkers van de softwareleverancier onbeperkte toegang tot het geautomatiseerde systeem hebben. Dit moet uit oogpunt van informatiebeveiliging als onwenselijk worden beschouwd.

Uit de interviews kwam naar voren dat de SIAD op een aantal belangrijke punten ongeschreven regels hanteert. Zo zou er een bijzondere regeling bestaan voor de toegang tot de gegevens van collega's, parlementariërs en ministers. Ook zou er een ongeschreven regel zijn dat medewerkers de dossiers van familieleden of vrienden niet zelf behandelen. Deze regelingen en de procedures die daarbij worden gehanteerd zijn niet beschreven.

# 4 *Soft controls*

Onder *soft controls* worden beheersmaatregelen verstaan die gericht zijn op het bevorderen van een integere cultuur in een organisatie. Daarbij kan onder andere worden gedacht aan opleidingen en bijeenkomsten om waarden en normen regelmatig op een positieve manier onder de aandacht van het personeel te brengen. Bij *soft controls* ligt de nadruk niet op de (controle op de) naleving van regels, maar op het levend houden van de integriteit in een organisatie. Managers en bestuurders hebben een belangrijke voorbeeldfunctie te vervullen en dat betekent onder meer dat zij met *soft controls* om moeten kunnen gaan.

Uit ons onderzoek komt naar voren dat de SIAD slechts in beperkte mate *soft controls* heeft geïmplementeerd. De volgende maatregelen zijn voorbeelden van *soft controls* die worden toegepast:

1. de aflegging van de eed/belofte bij indiensttreding;
2. de aandacht voor integriteitsdilemma's tijdens sollicitatiegesprekken;
3. managementtraining voor teamleiders, waarbij aandacht wordt geschonken aan integriteit;
4. een module integriteit in de basistraining voor belastingpersoneel.

De eerste maatregel geldt voor al het personeel dat bij de SIAD in dienst treedt. De tweede maatregel is toegepast bij een sollicitatieprocedure voor douanepersoneel en geldt nog niet voor alle sollicitatiegesprekken.
De als derde maatregel genoemde managementtraining is alleen gegeven aan teamleiders en richt zich slechts ten dele op integriteit. Bij de vierde maatregel is op te merken dat de basistraining, die buiten werktijd wordt gegeven, niet door alle nieuwe medewerkers wordt gevolgd. Deze training strekt zich ook nog niet uit tot het bestaande personeel.

Naast de hiervoor genoemde beperkingen van de toegepaste *soft controls*, laat de SIAD ook andere mogelijkheden onbenut om *soft controls* in te zetten. Zo maakt de SIAD geen gebruik van de volgende mogelijkheden:

- gestructureerd aandacht besteden aan integriteit tijdens functioneringsgesprekken, werkoverleg en personeelsbijeenkomsten;
- integriteitsbewustwordingsprogramma's, om waarden en normen onder de aandacht van het personeel te brengen, maar ook om het inzicht in kwetsbaarheden te verhogen;

- dilemmatrainingen, waarbij medewerkers met elkaar in gesprek gaan over integriteitskwesties die tijdens het werk kunnen spelen;
- belevingsonderzoek houden, waarbij medewerkers en management gevraagd worden naar de opvattingen over integriteit;
- specifiek aandacht geven aan de voorbeeldrol van het management.

De SIAD heeft geen vertrouwenspersonen aangesteld. Vertrouwenspersonen kunnen een aanspreekpunt zijn voor medewerkers die in een beschermde sfeer van gedachten willen wisselen over integriteitskwesties. Ook kunnen vertrouwenspersonen als intermediair optreden als medewerkers (verdenkingen van) integriteitsinbreuken willen melden.

Verschillende geïnterviewden hebben tijdens ons onderzoek aangegeven dat het thema integriteit naar hun indruk niet leeft onder het personeel. Ook is er geen cultuur van elkaar aanspreken op gedrag. De inzet van *soft controls* kan bijdragen aan het 'levend houden' van waarden, normen en gedragsregels. Het bevordert bovendien een organisatiecultuur, waarin integriteit de nodige aandacht heeft en bespreekbaar is.

*Bewustzijn ten aanzien van informatiebeveiliging*

*Soft controls* zijn ook van belang voor de informatiebeveiliging, omdat de menselijke factor hierbij een bepalende rol speelt. Het bevorderen van beveiligingsbewustzijn bij alle SIAD-medewerkers is daarom een randvoorwaarde voor een effectieve informatiebeveiliging. Uit ons onderzoek blijkt echter dat de SIAD geen specifieke activiteiten ontplooit om het informatiebeveiligingsbewustzijn van medewerkers te vergroten. Tijdens de interviews hebben enkele SIAD-medewerkers erop gewezen dat er niet altijd voldoende oog is voor een zorgvuldige omgang met de waardevolle en gevoelige informatie, waarover de SIAD gelet op haar taak beschikt.

# 5 Interne controle en accountantscontrole

Interne controle en accountantscontrole zijn in het algemeen nodig voor de ordelijkheid en controleerbaarheid van het (financiële) beheer en leveren op die wijze een bijdrage aan de integriteit van de organisatie en aan de inperking van risico's op fraude en andere onregelmatigheden.
Daarnaast zijn interne controle en accountantscontrole meer specifiek van belang om de naleving van het integriteitsbeleid, gedragscode en integriteitsregels te beoordelen. De controles dienen te leiden tot conclusies over de naleving van het integriteitsbeleid. Als er aanbevelingen zijn gedaan, moet via *follow-up* rapportages in beeld worden gebracht hoe de implementatie daarvan plaatsvindt.
De beoordeling van de naleving van integriteitsmaatregelen kan deel uitmaken van de controles van het financieel beheer en van de jaarverslagen, maar een volledige beoordeling van het stelsel van integriteitszorg zal meestal een afzonderlijk onderzoek vereisen.

Uit ons onderzoek kwam naar voren dat de SIAD niet over een interne controlefunctionaris of –afdeling beschikt.
Verder is gebleken dat de Centrale Accountantsdienst (CAD) sinds 2007 geen onderzoek meer heeft uitgevoerd bij het Belastingkantoor. De belangrijkste reden hiervoor is de introductie van een nieuw geautomatiseerd informatiesysteem (SAP). De CAD beschikt niet over de expertise om onderzoek te kunnen doen naar dit systeem.

De CAD heeft op 29 april 2010 een rapport uitgebracht over de beoordeling van de effectiviteit van het systeem van interne beheersing van de Inspectie der Invoerrechten en Accijnzen (Douane). Dit rapport bevat verschillende passages die ingaan op aspecten van integriteit.
Zo bevat het rapport onder andere de volgende bevindingen:

- een systematisch en gestructureerd inzicht ontbreekt in de risico's voor de realisatie van doelstellingen;
- de Douane licht personeel onvoldoende in over het personeelsbeleid van het land Aruba, waaronder de gedragsregels uit de LMA;

- de Douane beschikt niet over een gedragscode die is toegespitst op haar activiteiten en taken;
- de Douane heeft een concept van een huishoudelijk reglement opgesteld, maar nog niet vastgesteld;
- ministers leggen nagenoeg geen disciplinaire maatregelen op aan ambtenaren voor het niet nakomen van arbeidsverplichtingen;
- de procedure voor het opleggen van een disciplinaire straf is bijzonder omslachtig en lang, omdat een landsbesluit nodig is, waarbij minister en Gouverneur betrokken zijn;
- omdat disciplinaire maatregelen niet (consistent) worden opgelegd, hebben de gedragsregels in de LMA weinig gezag en straalt de Douane geen duidelijk handhavend signaal uit naar de medewerkers.

Het rapport van de CAD gaat ook in op de management- en operationele stijl bij de Douane, die als overwegend directief en streng wordt gekenschetst. Er wordt weinig gebruik gemaakt van de mogelijkheid van participatie en inbreng door het personeel. Onder het Douanepersoneel is er soms angst om (structurele) problemen aan te kaarten bij leidinggevenden, waardoor ze niet worden aangepakt.

Deze bevindingen van de CAD wijzen op gebreken in de organisatiecultuur, die verband houden met een onvoldoende inzet of werking van *soft controls* (zie hoofdstuk 4).

De CAD heeft tot op heden geen specifieke integriteitsaudit uitgevoerd bij de SIAD. Ook heeft de CAD geen IT audits verricht om onder andere de maatregelen van informatiebeveiliging te toetsen. Ten tijde van de uitvoering van ons onderzoek in juni 2012 verkeerde de SIAD in het proces van opdrachtverlening voor een IT audit. De resultaten van deze audit waren bij de afsluiting van ons onderzoek nog niet bekend.

# 6 Response bij mogelijke integriteitsbreuken

## 6.1 Signalen en meldingen

Medewerkers moeten signalen van (mogelijke) integriteitsinbreuken intern kunnen melden. Daarvoor dient een meldingsregeling te bestaan, ook wel aangeduid als 'klokkenluidersregeling'. Helder moet zijn bij wie medewerkers hun melding kunnen doen, onder welke voorwaarden een melding dient plaats te vinden en welke bescherming de melder geniet.

De SIAD blijkt niet te beschikken over een interne regeling voor het melden van (verdenkingen van) integriteitsinbreuken. Meer specifiek stellen we ten aanzien van de informatiebeveiliging vast dat de SIAD ook geen procedure kent voor het melden van beveiligingsincidenten. Zoals in hoofdstuk 4 al vermeld, beschikt de SIAD niet over vertrouwenspersonen die een intermediaire rol kunnen spelen bij het melden van (mogelijke) inbreuken.

Voor meldingen van externen heeft de SIAD een klachtenregeling. Deze regeling is bedoeld voor klachten over de bejegening door SIAD ambtenaren en niet specifiek voor het melden van (mogelijke) integriteitsinbreuken, maar kan daarvoor wel gevolgd worden.
Bij de klachtenregeling is een kanttekening te plaatsen ten aanzien van de geheimhouding van informatie die afkomstig is van de klager. In de folder uit 2009 over de klachtenprocedure belooft de SIAD alle informatie die de klager verstrekt geheim te houden. Deze belofte zal echter niet altijd waar te maken zijn. In het geval dat een klager een klacht indient die neerkomt op een strafbaar feit, moet de SIAD daar aangifte van kunnen doen, met als gevolg dat de identiteit van de klager niet geheim kan worden gehouden.

Voor (verdenkingen van) integriteitsinbreuken die strafbaar zijn gesteld in het Wetboek van strafrecht kan aangifte worden gedaan bij de politie of het Openbaar Ministerie. Voor bepaalde misdrijven geldt een aangifteplicht op grond van artikel 200 Wetboek van Strafvordering. Dit artikel bepaalt dat openbare colleges of ambtenaren verplicht zijn onverwijld aangifte te doen bij de (hulp)officier van justitie van:

- ambtsmisdrijven als genoemd in titel XXVIII van het Tweede Boek van het Wetboek Strafrecht;
- misdrijven waarbij een bijzondere ambtsplicht is geschonden of waarbij gebruik is gemaakt van macht, gelegenheid of middel door het ambt geschonken;
- misdrijven waarbij inbreuk of onrechtmatig gebruik is gemaakt van een regeling waarvan de uitvoering of de zorg voor de naleving tot de ambtstaak behoort.

In een brief van 19 april 1999 van de minister van Algemene Zaken is aangegeven dat een ambtenaar (vermoedens van) misdrijven dient te melden bij zijn directeur of diensthoofd, die dan vervolgens aangifte zal doen bij de officier van justitie. Als het (vermoeden van een) misdrijf de directeur of het diensthoofd zelf betreft, dient direct bij de officier van justitie aangifte te worden gedaan.
Deze brief van de minister van Algemene Zaken geldt voor de gehele overheidssector en dus ook voor de SIAD. De SIAD heeft geen nadere richtlijnen voor het doen van aangifte als er sprake is van strafbare feiten, waarvoor de aangifteplicht niet van toepassing is.

## 6.2 Onderzoek van signalen en meldingen

Meldingen van (mogelijke) integriteitsinbreuken of beveiligingsincidenten dienen te worden onderzocht en eveneens worden geanalyseerd op reikwijdte, verspreidingsgraad, omvang en oorzaken. Dit is nodig om de organisatie in staat te stellen lering te trekken uit incidenten. Ook als er aangifte is gedaan van strafbare feiten, kan er daarnaast aanleiding zijn om intern onderzoek te doen met het oog op te treffen rechtspositionele of disciplinaire maatregelen. In een zogeheten onderzoeksprotocol behoren de kaders voor de uitvoering van onderzoeken naar (verdenkingen van) integriteitsinbreuken te zijn vastgelegd. Een dergelijk protocol maakt onder andere helder wie beslist over het onderzoek, welke instrumenten bij het onderzoek kunnen worden ingezet en welke rechten en plichten daarbij gelden.

Uit ons onderzoek blijkt dat de SIAD niet beschikt over een onderzoeksprotocol. Afhankelijk van het incident, wordt ad hoc bepaald hoe het onderzoek moet plaatsvinden en wie het zal uitvoeren. Daardoor is onzeker of het onderzoek met voldoende reikwijdte en diepgang wordt uitgevoerd.

Om het onderzoek effectief te kunnen uitvoeren, zullen soms zogeheten ordemaatregelen nodig zijn, zoals het schorsen van personeel tijdens het onderzoek en het ontzeggen van de toegang tot de werkplek. Er is een beschrijving aanwezig van de procedure voor het ontzeggen van toegang aan een medewerker. Omdat in deze procedure is voorzien dat de minister hierover beslist, is een spoedige implementatie van ordemaatregelen vaak niet mogelijk. Er kunnen echter wel dringende redenen zijn om onmiddellijk tot deze maatregelen over te gaan, bijvoorbeeld om bewijsmateriaal

veilig te stellen. De gevolgde procedure kan daardoor een effectief onderzoek van integriteitsinbreuken hinderen.

Niet specifiek voor de SIAD, maar voor de gehele overheid, bestaat er sinds 22 augustus 2006 een protocol voor de informatieverstrekking door het OM aan de personeelsdiensten van de overheid. Het protocol betreft regels voor de informatieverstrekking door het OM als een ambtenaar of arbeidscontractant verdacht wordt van of is veroordeeld voor het plegen van een strafbaar feit en bezien moet worden of er aanleiding is tot het treffen van rechtspositionele of disciplinaire maatregelen.

## 6.3 Registratie van meldingen en inbreuken

De organisatie dient een ordelijke en actuele (centrale) registratie bij te houden van meldingen van (mogelijke) integriteitsinbreuken en van de (uitkomsten van de) onderzoeken naar deze meldingen. De registratie heeft tot doel om het management inzicht te verschaffen over de aard en omvang van de incidenten en over de (tijdige) afwikkeling daarvan. Daaruit kunnen patronen worden afgeleid en lessen worden getrokken om toekomstige inbreuken te voorkomen. Bovendien kan de registratie worden betrokken bij de externe verantwoording over integriteitszorg, bijvoorbeeld in het jaarverslag.

Bij de SIAD ontbreekt een gestructureerde registratie van meldingen en onderzoeken. Van disciplinaire zaken wordt per incident een dossier gevormd. Een overkoepelende registratie ontbreekt echter. De Douane houdt wel een spreadsheet bij van openstaande rechtspositionele aangelegenheden, die nog op een beslissing van de minister wachten. Dit spreadsheet verschaft enige informatie over de voortgang van de lopende disciplinaire zaken, maar geeft geen (statistisch) beeld van de meldingen, integriteitsinbreuken en bestraffingen.
Ook voor informatiebeveiligingsincidenten ontbreekt een ordelijke en actuele registratie van incidenten.

## 6.4 Disciplinaire straffen

Voor de toepassing van disciplinaire straffen dient een heldere procedure te bestaan. Deze procedure dient waarborgen te omvatten voor een zorgvuldige en effectieve bestraffing bij plichtsverzuim. Een organisatie dient ook een registratie bij te houden van de disciplinaire bestraffingen, als onderdeel van de managementinformatie voor het integriteitsbeleid.

De basis voor disciplinaire bestraffingen is te vinden in de LMA, in het bijzonder de artikelen 82 tot en met 86. De procedure voor de disciplinaire bestraffing is uitgeschreven in hoofdstuk 11 van het handboek DPO van 27 juli 2007. Daaruit blijkt dat de procedure een groot aantal stappen omvat en de besluitvorming over de strafoplegging plaats moet vinden op het niveau van minister en Gouverneur. Op grond van artikel 87, lid 2 kan het bevoegde gezag de bevoegdheid tot het opleggen van de drie lichtste vormen van disciplinaire bestraffing overdragen aan daartoe aan te wijzen functionarissen, maar dit is niet gebeurd.
De CAD besteedt in zijn rapport over de Douane van 29 april 2010 ook aandacht aan de procedure van disciplinaire bestraffingen (zie hoofdstuk 5) en typeert deze procedure als omslachtig en traag. Tijdens ons onderzoek hebben wij gesproken met SIAD-medewerkers die betrokken zijn bij de behandeling van disciplinaire zaken. Deze gesprekken bevestigen het beeld dat de procedure voor disciplinaire bestraffingen veel tijd vergt.

Artikel 84 van de LMA omvat een waarborg voor een zorgvuldige toepassing van disciplinaire straffen, namelijk dat de ambtenaar in de gelegenheid wordt gesteld zich te verantwoorden tegenover de tot het opleggen van straffen bevoegden. Daarvoor geldt een termijn van zeven dagen na kennisgeving van het voornemen om een disciplinaire straf op te leggen. Deze termijn van zeven dagen is kort, zeker als het om meer complexe zaken gaat. De LMA stelt geen termijn aan het bevoegd gezag om te besluiten over het voornemen om een disciplinaire straf op te leggen. Uit mededelingen van een ervaren medewerker Personeel en Organisatie (P&O) hebben wij begrepen dat een termijn van maximaal één jaar wordt aangehouden om het voornemen van een disciplinaire straf aan betrokkene mede te delen, omdat anders in redelijkheid geen verantwoording meer gevraagd kan worden. Deze termijn is echter niet in regelgeving verankerd.
Tegen het uiteindelijke besluit om een disciplinaire straf op te leggen, kan betrokkene binnen dertig dagen bezwaar aantekenen bij de ambtenarenrechter op grond van titel III van de Landsverordening regeling ambtenarenrechtspraak.

Bij de SIAD ontbreekt een registratie van disciplinaire bestraffingen. Dit is in lijn met de bevindingen ten aanzien van de registratie van meldingen en onderzoeken (zie § 6.3).
Door het ontbreken van een registratie kan de SIAD geen overzicht geven van het aantal en de aard van de disciplinaire bestraffingen. Tijdens de interviews in het kader van ons onderzoek hebben enkele respondenten, op basis van hun kennis van individuele gevallen, indicaties afgegeven van het gemiddelde aantal disciplinaire zaken per jaar. Hoewel de indicaties enigszins uiteenlopen, gaat het volgens alle respondenten om een beperkt aantal disciplinaire zaken per jaar. Bij de Belastingdienst betreft het slechts enkele (minder dan vijf) disciplinaire zaken per jaar en bij de Douane gaat het volgens de ruimste schatting om vijf à tien gevallen per jaar. Deze aantallen geven uiteraard slechts een indicatie van het aantal disciplinaire zaken en geen indicatie van

alle integriteitsinbreuken. Er is op grond van ons onderzoek geen uitspraak mogelijk over het aantal incidenten dat niet wordt gemeld of over het aantal incidenten dat na een melding niet in onderzoek wordt genomen, respectievelijk niet tot een disciplinaire bestraffing leidt.

# 7 Conclusies en aanbevelingen

## 7.1 Conclusies

De hoofdconclusie van ons onderzoek, en tevens het antwoord op de probleemstelling, is dat het stelsel van integriteitszorg van de SIAD niet toereikend is. Zo zijn er gebreken in de structuur en duurzaamheid van de integriteitszorg en is er weinig aandacht voor het bevorderen van een integere cultuur. Verder zijn er lacunes in de integriteitsregels, in het toezicht op de naleving van integriteitsregels en in de response bij (mogelijke) integriteitsinbreuken.

Voor een organisatie als de SIAD zijn gebreken in de integriteitszorg van zwaarwegend belang, omdat de SIAD zich bezig houdt met publieke taken, zoals belastingheffing en douanetaken, die inherent een hoog integriteitsrisico hebben. Zo zijn de (financiële) belangen voor belastingplichtigen groot en is binnen de SIAD veel vertrouwelijke informatie aanwezig. Daarnaast verkeerde de SIAD ten tijde van het onderzoek in een reorganisatie- en veranderingsproces, waardoor integriteitsrisico's verhoogd worden, bijvoorbeeld omdat de loyaliteit van personeel onder druk kan komen te staan.

Onze hoofdconclusie werken we als volgt uit in (deel)conclusies.

*Structuur en duurzaamheid van integriteitszorg*
Er zijn gebreken in de structuur en duurzaamheid van het stelsel van integriteitszorg bij de SIAD. Zo is er geen gestructureerde analyse van de integriteitsrisico's of van de risico's voor de informatiebeveiliging. Een uitgeschreven integriteitsbeleid en informatiebeveiligingsbeleid ontbreken. Voor zover maatregelen zijn getroffen, is dit vaak naar aanleiding van incidenten en daardoor reactief van karakter.
Er is ook geen sprake van een verantwoording over de uitvoering van integriteits- en informatiebeveiligingsbeleid of van een evaluatie daarvan. In het algemeen heeft de SIAD de afgelopen jaren geen externe verantwoording (jaarverslag) uitgebracht. Dit betekent dat er ook geen verantwoording is over het gevoerde integriteits- en informatiebeveiligingsbeleid.
Resumerend is het beeld dat de SIAD op het gebied van integriteitszorg en informatiebeveiliging geen beleidscyclus kent. Dit leidt ertoe dat het beleid onvoldoende van de grond komt en eventuele initiatieven weer gemakkelijk verwateren en daardoor geen duurzaam effect hebben.

*Cultuur*

Binnen de SIAD is er weinig aandacht voor preventie van integriteitsinbreuken en voor het bevorderen van een integere cultuur. De SIAD heeft bijvoorbeeld geen gedragscode vastgesteld en slechts in beperkte mate *soft controls* geïmplementeerd. Zo is er weinig aandacht voor het onderwerp integriteit tijdens functioneringsgesprekken of werkoverleg. Ook ontbreken bewustwordingsprogramma's, dilemmatrainingen en belevingsonderzoek. Er is te weinig aandacht voor de voorbeeldrol van het management. In de praktijk blijft bij de SIAD onderbelicht dat integriteitszorg vooral een managementverantwoordelijkheid is en niet in de eerste plaats de verantwoordelijkheid van de afdeling Personeel & Organisatie. Voor de informatiebeveiliging kunnen soortgelijke conclusies worden getrokken als voor de integriteitszorg in het algemeen.

Er worden geen specifieke activiteiten ontplooid om het informatiebeveiligingsbewustzijn te verbeteren. Daardoor kunnen medewerkers het beeld hebben dat de IT-afdeling de informatiebeveiliging volledig regelt en kunnen medewerkers hun eigen rol in dit kader onderschatten. Ook blijft onderbelicht dat de primaire verantwoordelijkheid voor informatiebeveiliging bij het management ligt en niet bij de IT-afdeling.

*Integriteitsregels en toezicht*

Voor zover de SIAD het stelsel van integriteitszorg heeft ingevuld, ligt de nadruk vooral op integriteitsregels, waaraan het personeel zich heeft te houden.

Ondanks de aandacht voor integriteitsregels, concluderen we dat er op onderdelen lacunes bestaan:

- De SIAD heeft geen regels die moeten voorkomen dat uit dienst tredend personeel direct of binnen een korte termijn weer wordt ingehuurd als extern adviseur (tegengaan van 'draaideurconstructies'). Ook zijn er geen integriteitsregels gesteld om intimidatie, discriminatie en andere ongewenste omgangsvormen op de werkplek tegen te gaan.
- De regeling voor nevenarbeid dekt niet alle ongewenste nevenbelangen af. Er is geen bepaling die het ambtenaren verbiedt om (financiële) nevenbelangen, anders dan nevenarbeid, aan te gaan of aan te houden, die in strijd (kunnen) komen met een goede functievervulling.
- De Belastingdienst hanteert een geschenkenregeling waarin een waardegrens is aangegeven (maximaal Afl. 50); dit betekent dat een gift in de relatie tussen belastingplichtige en Belastingdienst niet onder alle omstandigheden wordt afgewezen.
- De SIAD heeft geen samenhangend pakket van beveiligingsmaatregelen vastgesteld om inbreuken op de vertrouwelijkheid van de informatie te voorkomen.
- Op een aantal belangrijke punten hanteert de SIAD ongeschreven regels, zoals voor de toegang tot gevoelige dossiers, die geformaliseerd zouden moeten zijn.

De controle en het toezicht op de naleving van integriteitsregels zijn onvoldoende. De SIAD beschikt niet over een interne controlefunctionaris of –afdeling. De CAD

heeft al jaren geen onderzoek meer uitgevoerd bij het Belastingkantoor. Het meest recente CAD-rapport van april 2010 over de Douane wijst op tekortkomingen op het gebied van de integriteitszorg. De CAD heeft geen specifieke integriteitsaudits uitgevoerd bij de SIAD. Ook heeft de CAD geen IT audits verricht om onder andere de maatregelen van informatiebeveiliging te toetsen.

*Response bij mogelijke integriteitsinbreuken*
Binnen de SIAD is er geen meldingsregeling voor medewerkers die een (mogelijke) integriteitsinbreuk intern willen melden. Er is wel een (externe) klachtenregeling, maar de geheimhouding die in een folder over de klachtenregeling wordt beloofd aan de melders, is niet onder alle omstandigheden waar te maken. De SIAD heeft geen heldere richtlijnen voor het doen van aangifte bij (verdenking van) strafbare feiten, in die gevallen dat er geen wettelijke aangifteplicht is.

De SIAD beschikt niet over een protocol voor het onderzoek naar (mogelijke) integriteitsinbreuken of informatiebeveiligingsincidenten. De slagvaardigheid bij het treffen van ordemaatregelen, zoals het ontzeggen van toegang tot de werkplek, is beperkt, omdat daarvoor een beslissing van de minister nodig is. De beslissing om een disciplinaire straf op te leggen is, ook bij de lichtste vormen van bestraffing, voorbehouden aan minister en Gouverneur en voor deze beslissing is er geen uiterste termijn gesteld. Daarentegen is bij voorgenomen disciplinaire bestraffingen de termijn voor de ambtenaar om zich te verantwoorden zeer kort, namelijk zeven dagen. In de praktijk is de procedure van disciplinaire bestraffing omslachtig en traag, waardoor de effectiviteit en geloofwaardigheid van disciplinaire straffen onder druk komt te staan.
Tot slot ontbreekt bij de SIAD een gestructureerde registratie van meldingen, onderzoeken en bestraffingen. Ook is er geen registratie van incidenten op het terrein van informatiebeveiliging.

## 7.2 Aanbevelingen

Op grond van de resultaten van ons onderzoek, bevelen we de minister belast met Financiën aan om de volgende maatregelen uit te (laten) werken:

- Versterk het beleidskader en de beleidscyclus voor de integriteitszorg en informatiebeveiliging structureel:
  - Formuleer een integriteitsbeleid en informatiebeveiligingsbeleid, waarin doelen, uitgangspunten en maatregelen zijn vastgelegd en dat uitgaat van een complete beleidscyclus (formuleren, uitvoeren, evalueren en bijstellen van beleid).
  - Voer ter onderbouwing van het beleid periodieke risicoanalyses uit om integriteits- en beveiligingsrisico’s te signaleren en te analyseren. Verwerk de resultaten van deze analyses in (de actualisering van) het integriteits- en informatiebeveiligingsbeleid.

- Leg ten minste jaarlijks verantwoording af over de uitvoering van het beleid. De SIAD dient verantwoording af te leggen aan de minister en de minister dient op zijn beurt verantwoording af te leggen aan het Parlement.
- Laat het beleid periodiek (bijvoorbeeld eens in de drie of vier jaar) evalueren om het beleid bij te sturen en om het beleid een duurzaam en structureel karakter te geven.

- Benadruk de primaire verantwoordelijkheid en de voorbeeldrol van management voor integriteitszorg en informatiebeveiliging en voorkom dat deze onderwerpen vooral als een verantwoordelijkheid van de afdelingen P&O, respectievelijk ICT worden beschouwd.
- Investeer in *soft controls*, zoals het formuleren van een gedragscode, het aanstellen van vertrouwenspersonen, het verzorgen van (dilemma)trainingen en bijeenkomsten, het verrichten van belevingsonderzoek, het uitvoeren van bewustwordingsactiviteiten voor informatiebeveiliging en gerichte communicatie over integriteitsonderwerpen. Het is van belang dat deze investeringen een duurzaam en niet een eenmalig karakter hebben, omdat een integere en veilige cultuur in een organisatie voortdurend onderhoud vergt.
- Vul de bestaande integriteitsregels en –procedures aan om lacunes weg te nemen. Daarbij gaat het om regelingen ter voorkoming en bestrijding van 'draaideurconstructies', intimidatie, discriminatie en ongewenste nevenbelangen (anders dan nevenarbeid). De geschenkenregeling is aan te scherpen door niet toe te laten dat geschenken, ook wanneer ze een geringe financiële waarde hebben, worden geaccepteerd van belastingplichtigen. Stel ook een samenhangend pakket van regels en maatregelen vast voor de informatiebeveiliging en voor de omgang met gevoelige dossiers.
- Introduceer periodieke audits op het terrein van integriteit en informatiebeveiliging. Dit zijn specifieke gerichte audits die aanvullend zouden moeten zijn op de interne controle binnen de SIAD en op (externe) audits van de financiële verantwoordingen en van het financiële en operationele beheer bij de SIAD.
- Versterk de instrumenten voor de response bij (mogelijke) integriteitsinbreuken:
  - Formaliseer een interne regeling voor het melden van (verdenkingen van) integriteitsinbreuken of beveiligingsincidenten en informeer alle medewerkers hierover.
  - Stel een protocol vast voor onderzoek naar (mogelijke) integriteitsinbreuken en informatiebeveiligingsincidenten.
  - Stel een heldere richtlijn vast voor het doen van aangifte bij (verdenking van) strafbare feiten, in die gevallen dat er geen wettelijke aangifteplicht is.
  - Zorg voor een gestructureerde registratie van meldingen, incidenten, onderzoeken en bestraffingen.

Tot slot bevelen we de minister van Financiën aan om het treffen van ordemaatregelen en het opleggen van disciplinaire maatregelen, in ieder geval de lichtere vormen van disciplinaire bestraffing [6], naar de hoogste ambtelijke leiding van de SIAD te mandateren. Dit ter bevordering van de slagvaardigheid en geloofwaardigheid van disciplinaire maatregelen.

[6] Zie artikel 87, lid 2 van de LMA.

# 8 Reactie minister van Financiën en nawoord Algemene Rekenkamer

Op 2 november 2012 heeft de minister van Financiën gereageerd op ons conceptrapport. Zijn reactie geven we hierna integraal weer.

*Bestuurlijke reactie minister*

"Ik heb kennis genomen van uw conceptrapport, met dagtekening 28 september 2012, met betrekking tot het onderzoek naar het stelsel van integriteitszorg bij de SIAD. In dit verband treft u onderstaand mijn reactie op het voornoemd rapport.

Allereerst zou ik mijn verontwaardiging willen uiten over het feit dat de stellingen en aannames in het rapport grotendeels gebaseerd zijn op interviews en niet zo zeer op feitelijke bevindingen, zoals een overzicht in de literatuurlijst van de relevante stukken die ten grondslag liggen aan de stellingen.

U concludeert dat voor een organisatie als de SIAD gebreken in de integriteitszorg van zwaarwegend belang zijn, omdat de SIAD zich bezighoudt met publieke taken die inherent een hoog integriteitsrisico hebben. U geeft als voorbeeld aan dat gezien het feit dat de SIAD ten tijde van het onderzoek in een reorganisatie- en veranderingsproces verkeerde de integriteitsrisico's verhoogd worden.

Gevolggevend aan de moties van de Staten van Aruba van 30 december 2009 om onderzoek te verrichten naar het functioneren van de SIAD heb ik in het vierde kwartaal van het jaar 2010 een Performance Quick Scan laten uitvoeren door KPMG Advisory Services N.V.

Naar aanleiding van de door KPMG gesignaleerde knelpunten in de bedrijfsvoering van de SIAD heb ik d.d. 16 november 2010 een Management Team ingesteld bij de SIAD (hierna: MT SIAD). Het MT SIAD is belast geweest met het doen van onderzoek naar de knelpunten binnen de bedrijfsvoering van de SIAD en is belast met het opstellen van een verbeterplan. Het is mij onduidelijk of in dit

conceptrapport de bevindingen van KPMG en het MT SIAD zijn meegenomen in uw onderzoek.

De bevindingen van het onderzoek van het MT SIAD zijn vastgelegd in een interim rapport gedagtekend 23 mei 2011. Uit dit rapport vloeit voort dat de bedrijfsvoering van de SIAD structureel verbeterd dient te worden wil de SIAD zich ontwikkelen tot een professionele organisatie die streeft naar handhaving van rechtszekerheid en rechtsgelijkheid dat zich onder andere uit in een transparante, flexibele, klantvriendelijke, betrouwbare, zorgvuldige, verantwoordelijke, efficiënte en doelmatige organisatie. Naar de klant toe dient te SIAD conform te actualiteit te functioneren op operationeel, IT en fiscaal gebied. Teneinde het verbeterplan op te kunnen stellen is een verbetertraject gestart bestaande uit elf deelprojecten met bijstand van externe partijen. Dit verbetertraject is op dit ogenblik volledig in uitvoering.

Ik heb op basis van de conclusies en aanbevelingen van het interim rapport van het MT SIAD besloten om een aantal structurele veranderingen aan te brengen binnen de SIAD organisatie in de vorm van de verzelfstandiging van de Servicio di Impuesto en de Servicio di Aduana van de Directie der Belastingen. Het voornoemd veranderproces is reeds aangevangen, waarbij de laatste gelijktijdig wordt opgeheven.

Uw conclusie dat de belastingdienst in een reorganisatie- en veranderingsproces verkeerde en dat ten gevolge daarvan de integriteitsrisico's verhoogd worden is uitermate voorbarig. Het voornoemd reorganisatie- en veranderingsproces is juist in gang gebracht om de integriteitsrisico's weg te nemen.

U concludeert dat de SIAD geen regels heeft die moeten voorkomen dat uit dienst treden personeel direct of binnen korte termijn weer wordt ingehuurd als extern adviseur personeel direct of binnen een korte termijn weer worden ingehuurd als externe adviseur (tegengaan van draaideurconstructies). Voor zover mij bekend is dit verschijnsel bij de SIAD slechts een enkele keer voorgekomen. Voor zo'n klein eiland als Aruba met een beperkt aanwezige expertise is het de vraag of een desbetreffende beperking wel haalbaar of gewenst is.

Tevens concludeert u dat de regeling voor nevenarbeid niet alle ongewenste nevenbelangen afdekt. Het is niet ongebruikelijk dat het bevoegd gezag de beslissing neemt of een bepaalde nevenactiviteit wel of niet mag worden uitgevoerd. Een algeheel verbod zou inhouden dat er met individuele gevallen geen rekening wordt gehouden. Zo zou een ambtenaar geen bestuursfunctie kunnen bekleden in een culturele, charitatieve en sportinstelling of als vrijwilliger kunnen optreden, of zelfs als gastdocent cursussen bij onderwijsinstellingen verzorgen.

Bovendien wordt dit zelfs niet in het licht van de gedragscodes voor privaatrechtelijke rechtspersonen als ongewenst aangemerkt. Verder zou het wel heel vergaand zijn als een ambtenaar van de belastingdienst geen lening meer zou kunnen aangaan, geen credit card etc. Ook Nederlandse belastingambtenaren hebben leningen, credit cards, hypotheken en dergelijke.

Voorts concludeert u dat de huidige geschenkenregeling van de SIAD (maximaal Afl. 50) impliceert dat een gift in de relatie tussen belastingplichtige en belastingdienst niet onder alle omstandigheden wordt afgewezen. De SIAD heeft een geschenkenregeling opgesteld teneinde een onduidelijkheid in artikel 59 van de LMA te verhelderen. De SIAD heeft daarom aanvullende regels opgesteld met een waardegrens, heeft kaders aangegeven voor de openheid en het type giften. Het is in andere landen niet ongebruikelijk om een gift aan ambtenaren, mits het beneden een bepaalde waarde blijft niet als ontoelaatbare gift te beschouwen. Derhalve is het mij niet geheel duidelijk waarom bij deze regeling een kanttekening geplaatst dient te worden. Uiteraard ben ik open voor suggesties uwerzijds.

In uw conceptrapport merkt u op dat uit interviews in het kader van uw onderzoek naar voren is gekomen dat externe medewerkers van de softwareleveranciers onbeperkte toegang tot het geautomatiseerde systeem hebben en dat dit uit oogpunt van informatiebeveiliging als onwenselijk moet worden beschouwd. Het laatste is ook mijn grote zorg geweest bij mijn aantreden als minister van het kabinet Mike Eman. Inmiddels heeft de SIAD het contract met deze softwareleverancier opgezegd en zal nu worden overgegaan tot het opzetten van een intern beheerde competence center.

Verder constateert u dat er lacunes zijn in de informatiebeveiliging bij de SIAD. Het MT SIAD is juist door mij aangesteld om een verbeterplan op te stellen op het gebied van informatietechnologie. Een van de deelprojecten van het verbetertraject is het uitvoeren van een IT-audit. De IT-audit is inmiddels bijna afgerond en er zijn reeds nieuwe verbeterde processen in gang gebracht.

Tenslotte stelt u dat de SIAD niet beschikt over een protocol voor het onderzoek naar (mogelijke) integriteitsinbreuken of informatiebeveiligingsincidenten. U vervolgt door te stellen dat de slagvaardigheid bij het treffen van ordemaatregelen, zoals het ontzeggen van de toegang tot de werkplek, beperk is, omdat daarvoor een beslissing van de minister nodig is. Ik wil hierbij opmerken dat ik in het geval van het informatielekincident van vorig jaar direct heb ingegrepen door de toegang te ontzeggen van de personen met eventuele betrokkenheid bij het incident en direct een onderzoek heb laten verrichten naar deze informatielek, opdat het bewijsmateriaal gewaarborgd bleef. Derhalve heeft de door de LMA vastgestelde procedure het onderzoek niet verhinderd.

Met betrekking tot uw aanbevelingen wens ik op te merken dat in het strategisch beleidsplan van de belastingdienst en het douanekantoor er rekening zal worden gehouden met het bevorderen van de integriteit binnen de dienst. Uw rapport zal ook gebruikt worden als bijdrage bij de implementatie van nieuw beleid inzake integriteit en informatiebeveiliging."

*Nawoord Algemene Rekenkamer*

De Algemene Rekenkamer waardeert het dat de minister in het strategisch beleidsplan rekening zal houden met het bevorderen van de integriteit van de dienst en ons rapport zal gebruiken bij de implementatie van nieuw beleid inzake integriteit en informatiebeveiliging. De minister laat in zijn reactie in het midden hoe en wanneer hij onze aanbevelingen gaat implementeren. Wij raden de minister aan de Staten concreet te laten weten hoe hij de aanbevelingen gaat implementeren en wanneer de resultaten zichtbaar zullen zijn.

Wij besteden aandacht aan de specifieke opmerkingen van de minister. Wij lichten daarbij enkele misverstanden toe.

- In zijn reactie stelt de minister dat ons rapport grotendeels op interviews gebaseerd zou zijn. Uit ons rapport is evident dat deze zienswijze niet correct is. In het rapport hebben we namelijk verwezen naar relevante documentatie. Echter een belangrijke conclusie van ons onderzoek is juist dat bij de SIAD veel documentatie ontbreekt.
- De minister plaatst ook enkele kanttekeningen bij onze opmerking over verhoogde integriteitsrisico's tijdens het lopende reorganisatie- en veranderingsproces. De ervaring heeft geleerd dat organisaties juist tijdens dergelijke trajecten kwetsbaarder zijn voor integriteitsinbreuken. Met ons rapport hebben wij de minister bewuster willen maken van deze risico's en dus van het belang en de urgentie van de implementatie van een goed stelsel van integriteitszorg.
- De minister vraagt zich af of beperking van draaideurconstructies voor een klein eiland als Aruba wel haalbaar of gewenst is. Wij zijn van mening dat de kleinschaligheid van Aruba juist de kwetsbaarheid op dit punt verhoogt. Ambtenaren met specifieke deskundigheid kunnen hun schaarste op deze manier gemakkelijk uitbuiten, ook al is dat volgens de minister bij de SIAD weinig voorgekomen. Zo hebben wij bij ons onderzoek naar personeel binnen de overheid, waarover wij in ons jaarverslag 2000-2004 gerapporteerd hebben, vastgesteld dat het omzetten van een dienstverband in een arbeidscontract zich binnen de publieke sector regelmatig voordoet.
- De minister lijkt uit ons rapport te hebben begrepen dat wij alle nevenactiviteiten en nevenbelangen van ambtenaren afwijzen. Wij doelen echter alleen op nevenactiviteiten en nevenbelangen die (kunnen) conflicteren

met de hoofdfunctie, waarvoor verdergaande regelingen getroffen moeten worden.

- Met onze opmerkingen over de geschenkenregeling bij de SIAD willen wij erop wijzen dat een grensbedrag niet absoluut gehanteerd kan worden. Onder bepaalde omstandigheden, bijvoorbeeld tijdens de behandeling van een aangifte van de belastingplichtige, is het accepteren van een gift (ook van een gering bedrag) niet acceptabel, vanwege de schijn van voorkeursbehandeling die daardoor kan ontstaan. Het behoort tot de kenmerken van een goede integriteitscultuur dat het vermogen aanwezig is om te beoordelen in welke situaties geschenken al dan niet aanvaardbaar zijn.
- Over het treffen van ordemaatregelen bij (verdenkingen van) integriteitsinbreuken merkt de minister op dat hij bij het incident in 2011 met het lekken van informatie snel heeft ingegrepen. Wij hebben echter geen (persoonsgericht) onderzoek naar dit incident gedaan. Ons onderzoek richtte zich op het stelsel van integriteitszorg en daarbij hebben we vastgesteld dat de procedure om te komen tot een dergelijke beslissing veel schakels omvat. Wij wensen met onze aanbeveling dan ook te bevorderen dat de daadkracht in alle gevallen waar sprake is van een (mogelijke) integriteitsbreuk waargemaakt kan worden.

Wij zouden het een goede zaak vinden als ons rapport ook een bredere impuls geeft aan de verbetering van de integriteitszorg bij andere onderdelen van de overheid, voor zover daar vergelijkbare lacunes zijn waar te nemen. De Algemene Rekenkamer is gaarne bereid om hier waar mogelijk een helpende hand te bieden. Wij zullen de ontwikkelingen op dit gebied, ook bij de SIAD, met aandacht blijven volgen.

# Bijlage 1: Methodologische verantwoording

In deze bijlage geven wij een toelichting op de aanpak en de methoden die zijn toegepast bij dit onderzoek. Achtereenvolgens gaan we in op de normen voor integriteitszorg, de onderzoeksvragen, de dataverzameling en de procedures van wederhoor.

**Normen voor integriteitszorg**

De integriteitszorg van overheidsorganisaties, zoals de SIAD, beoordelen we aan de hand van de volgende normen:[7]

1. Een overheidsorganisatie moet onkreukbaar en betrouwbaar zijn;
2. Een overheidsorganisatie moet beschikken over een analyse van de voor haar relevante integriteitsrisico's;
3. Bij een overheidsorganisatie behoort een basispakket aan maatregelen te zijn getroffen om inbreuken op de integriteit te voorkomen;
4. Bij een overheidsorganisatie dienen inbreuken op de integriteit door specifieke maatregelen te worden geneutraliseerd of beperkt;
5. Bij een overheidsorganisatie moet het integriteitsbeleid periodiek worden geëvalueerd;
6. De accountant of auditdienst van een overheidsorganisatie dient aandacht te besteden aan de naleving van het integriteitsbeleid.

*Ad. 1 Onkreukbaar en betrouwbaar zijn*

Het aangrijpingspunt voor de Algemene Rekenkamer is de institutionele integriteit van de overheid. Dit houdt in dat overheidsorganisaties onkreukbaar en betrouwbaar dienen te zijn. Integriteit is in die zin een element van behoorlijk bestuur. De integriteit van overheidsorganisaties dient ondersteund te worden door de individuele integriteit van functionarissen (bestuurders en ambtenaren) die binnen deze organisaties werkzaam zijn.

Integriteit heeft ook een relationele dimensie: zowel betrekkingen tussen overheidsorganisaties onderling (publiek-publiek) als tussen overheids-organisaties en derden (publiek-privaat) moeten integer van aard zijn. De achtergrond van deze laatste norm is dat een integere overheid geen banden mag hebben met organisaties die niet integer zijn.

*Ad. 2 Uitvoeren van een risicoanalyse*

Sommige werkgebieden, activiteiten of omstandigheden binnen een organisatie hebben een verhoogd risico, omdat ze kwetsbaar zijn voor integriteitsschendingen. Het is van belang de factoren te kennen die tot een verhoogd risico leiden, om te

[7] Deze normen zijn gebaseerd op een basisnormnotitie die de Algemene Rekenkamer van Nederland hanteert voor de Rijksoverheid in Nederland.

kunnen beoordelen welke (aanvullende) maatregelen getroffen moeten worden ter compensatie van het verhoogde risico. Hiertoe zal een risicoanalyse moeten worden uitgevoerd. In de risicoanalyse zullen alle kwetsbare werkgebieden/activiteiten en alle omstandigheden die de kwetsbaarheid van de betreffende organisatie voor integriteitsschendingen vergroten, betrokken moeten worden. Het resultaat van de analyse is een overzicht van risicoverhogende factoren met een aanduiding van de oorzaken daarvan.

*Ad. 3 Voorkomen van inbreuken*

Overheidsorganisaties moeten zich wapenen tegen dreigingen uit de omgeving die de eigen onkreukbaarheid zouden kunnen aantasten. Elke organisatie in de publieke sector heeft in meer of mindere mate te maken met integriteitsrisico's. Dit betekent ook dat elke organisatie een basispakket aan maatregelen dient te treffen om inbreuken op de integriteit te voorkomen.

*3.1 Integriteitsbeleid en gedragscode*

Overheidsorganisaties moeten beschikken over een integriteitsbeleid en een gedragscode. Deze behoren mede gebaseerd te zijn op de (specifieke) risicoanalyse. Het beleid en de gedragscode moeten de verplichtende elementen uit wet- en regelgeving omvatten.

Bij de totstandkoming van het integriteitsbeleid en de daarbij behorende risicoanalyse zouden management en medewerkers actief betrokken moeten zijn. Zij moeten onder meer de gelegenheid krijgen om risico's of dilemma's te signaleren. De gedragscode behoort normerend te zijn, in de zin dat er regels moeten zijn geformuleerd voor (on)aanvaardbaar gedrag en daarbij behorende sancties zijn aangegeven.

Voor de toetsing van de relevante integriteitsregels hebben wij in dit onderzoek de volgende *checklist* gehanteerd.

| **Regelgeving** |
| --- |
| ambtsmisdrijven (strafwet) |
| meldingsregeling incidenten ('klokkenluidersregeling') |
| regeling nevenfuncties, -verdiensten, -belangen |
| regeling acceptatie / geven van geschenken |
| tegengaan 'draaideurconstructies' |
| afleggen ambtseed/belofte |
| declaratieregelingen |
| (computer) informatiebeveiliging / *geheimhouding* |
| aanstelling vertrouwenspersonen:<br>- integriteit<br>- 'klokkenluiders'<br>- seksuele intimidatie/discriminatie |

| |
|---|
| kwetsbare functies / screening (*ook van externe relaties*) |
| regeling gebruik internet / eigendommen werkgever |
| regeling (ongewenste) omgangsvormen |

*3.2 Interne controlemaatregelen integriteitsbeleid en gedragscode*

In elke overheidsorganisatie moeten interne controlemaatregelen zijn getroffen die specifiek gericht zijn op de naleving van het integriteitsbeleid en de gedragscode.

*3.3 Monitoring van de resultaten interne controlemaatregelen*

Ten behoeve van het management van een overheidsorganisatie behoort monitoring plaats te vinden van de resultaten van de interne controlemaatregelen. Op basis daarvan dient aan het management te worden gerapporteerd.

*3.4 Aandacht voor soft controls*

Onder *soft controls* worden beheersmaatregelen verstaan die gericht zijn op het bevorderen van een integere cultuur in een organisatie. In elke organisatie dient er aandacht voor *soft controls* te zijn, zodat het integriteitsbewustzijn van medewerkers en managers op alle niveaus wordt gestimuleerd. De organisatie dient waarden en normen regelmatig onder de aandacht van het personeel te brengen, waardoor houding en gedrag van medewerkers positief worden beïnvloed. Managers en bestuurders hebben hierin een belangrijke voorbeeldfunctie te vervullen.

*Ad. 4 Inbreuken neutraliseren of beperken*

Als er sprake is van factoren die de integriteitsrisico's vergroten, moeten deze door de organisatie in kwestie geneutraliseerd of beperkt worden door specifieke maatregelen. Deze specifieke maatregelen behoren aanvullend te zijn op het basispakket van maatregelen.
Het beoordelen of specifieke maatregelen in een concrete situatie de bijzondere risico's afdoende compenseren, is maatwerk. Daarbij is het van belang om na te gaan of er sprake is van een uitgebalanceerd pakket van preventieve, detectieve en repressieve maatregelen.
Het ligt in eerste instantie het meest voor de hand dat de organisatie preventieve maatregelen treft. De risico's die kwetsbare omstandigheden met zich meebrengen kunnen immers het gemakkelijkst worden teruggedrongen door deze omstandigheden zélf te veranderen.

*4.1 Ordelijke en actuele registratie integriteitsinbreuken*

De organisatie dient een ordelijke en actuele (centrale) registratie bij te houden van meldingen van (mogelijke) integriteitsinbreuken. De meldingen moeten worden onderzocht en beoordeeld. De (mogelijke) inbreuken moeten eveneens

worden geanalyseerd op reikwijdte, verspreidingsgraad, omvang en oorzaken. De organisatie dient lering te trekken uit incidenten.

*4.2 Verdenking van strafbare feiten*

Wanneer er sprake is van een concrete verdenking van strafbare feiten, moet de leiding van de desbetreffende organisatie aangifte doen bij het Openbaar Ministerie.

*4.3 Sancties*

Sancties behoren in overeenstemming met de geldende criteria te worden toegepast. Op basis van het integriteitsbeleid en/of de gedragscode (zie 3.1) moeten disciplinaire straffen/sancties worden opgelegd aan overtreders.

*Ad. 5 Periodiek uitvoeren van een evaluatie*

Het integriteitsbeleid dient periodiek te worden geëvalueerd. De organisatie behoort zo nodig haar integriteitsbeleid aan te passen op basis van de evaluatieresultaten.

*Ad. 6 Aandacht besteden aan naleving integriteitsbeleid*

De accountant of auditdienst van de organisatie dient aandacht te besteden aan de naleving van het integriteitsbeleid. De onderzoeken van de accountant of auditdienst moeten leiden tot conclusies en aanbevelingen en de organisatie dient lering te trekken uit de onderzoeksresultaten.

**Onderzoeksvragen**

Voor het onderzoek is onderstaande lijst met vragen en aandachtspunten gehanteerd. Deze lijst is grotendeels gebaseerd op het onderzoekskader dat de Algemene Rekenkamer in Nederland heeft ontwikkeld voor integriteitsonderzoeken bij het Rijk. De beantwoording van de onderzoekvragen richt zich in hoofdzaak op de opzet en het bestaan in de praktijk van de maatregelen van integriteitszorg.

| **Integriteitsbeleid / gedragscodes** |
|---|
| Is een integriteitsbeleid geformuleerd? |
| Is een gedragscode aanwezig? |
| Zijn de in wet- en regelgeving verankerde integriteitsaspecten geïncorporeerd? |
| Zijn er (meetbare) doelstellingen voor integriteitsbeleid geformuleerd? |
| Was management betrokken bij de formulering van het integriteitsbeleid? |
| Waren medewerkers betrokken bij de formulering van het integriteitsbeleid? |
| Is het beleid gecommuniceerd naar de medewerkers? |
| Is integriteit onderdeel van functioneringsgesprekken en werkoverleg? |
| Wordt scholing en vorming aangeboden op het gebied van integriteit? |
| Zijn beleid / gedragscode gebaseerd op risicoanalyse? |
| Zijn aan beleid / gedragscode sancties gekoppeld? |
| **Beleidsevaluatie en verantwoording** |
| Is er een evaluatie van beleid en/of gedragscode? |

| |
|---|
| Komen conclusies / aanbevelingen uit de evaluatie voort?<br>Is er een follow-up rapportage?<br>Wordt verantwoording afgelegd over het gevoerde integriteitsbeleid?<br>Wordt verantwoording afgelegd over de naleving van de gedragscode? Zo ja, aan wie (democratisch orgaan, ondernemingsraad etc.)? |
| **Risicoanalyse** |
| Is een risicoanalyse aanwezig?<br>Was management betrokken bij de risicoanalyse?<br>Waren medewerkers betrokken bij de risicoanalyse? |
| **Interne controle op naleving integriteitsbeleid** |
| Zijn er interne controlemaatregelen getroffen specifiek gericht op het integriteitsbeleid?<br>Leveren de interne controlemaatregelen resultaten op? |
| **Accountantscontrole** |
| Besteedt de accountant specifiek aandacht aan (naleving van) integriteitsbeleid?<br>Komen conclusies / aanbevelingen voort uit de accountantscontroles?<br>Wordt er lering getrokken uit de controleresultaten?<br>Is er een follow-up rapportage? |
| ***Soft Controls*** |
| Besteedt de organisatie aandacht aan een integere cultuur en zogeheten *soft controls* en zo ja, hoe?<br>Wordt onderzoek gedaan naar de beleving van integriteit onder de medewerkers?<br>Wordt het integriteitsbewustzijn onder medewerkers en managers bevorderd en zo ja, hoe?<br>Brengt de organisatie waarden en normen regelmatig onder de aandacht van medewerkers en managers en zo ja, op welke wijze?<br>Besteedt de organisatie aandacht aan de voorbeeldfunctie van het management als het gaat om integriteit en zo ja, hoe? |
| **Meldingenregistratie** |
| Is er een registratie van meldingen van (mogelijke) inbreuken op de integriteit?<br>Is een registratie van inbreuken/schendingen aanwezig?<br>Bestaan hiervoor standaardprocedures? |
| **Onderzoek naar mogelijke inbreuken** |
| Wordt elke melding van een mogelijke integriteitsinbreuk onderzocht?<br>Bestaan hiervoor standaardprocedures? / *onderzoeksprotocol*<br>Zijn onderzoeksverslagen beschikbaar?<br>Worden de reikwijdte, omvang en oorzaken geanalyseerd?<br>Wordt lering getrokken uit incidenten?<br>Is er een follow-up rapportage? |
| **Aangifte bij Openbaar Ministerie** |
| Wordt bij verdenking van strafbare feiten aangifte gedaan? |
| **Disciplinaire straffen** |
| Is er een registratie van disciplinaire bestraffingen? |

### Dataverzameling

Voor het beantwoorden van de onderzoeksvragen hebben we allereerst gebruik gemaakt van documentanalyse. Wij hebben relevante documenten die gerelateerd zijn aan de integriteitszorg en informatiebeveiliging van de SIAD opgevraagd en

bestudeerd. Dit betreft onder andere beleidsdocumenten, risicoanalyses, gedragscodes, evaluaties en controlerapportages.
Naast de documentanalyse hebben wij ook interviews gehouden met een aantal sleutelfunctionarissen van de SIAD, het Ministerie van Financiën en de CAD.
Binnen de SIAD hebben wij met de volgende functionarissen gesproken:

- leden managementteam
- waarnemend directeur
- waarnemend hoofd Belastingkantoor
- hoofd Douane
- waarnemend manager IT
- teamleider Ondernemingen 2
- hoofd P&O
- medewerker P&O Douane
- controller
- projectadviseur bestuurlijke informatievoorziening

Daarnaast hebben wij met adviseurs van de minister van Financiën en de waarnemend directeur van de CAD gesproken, omdat zij vanuit hun eigen rol informatie kunnen geven over de integriteitszorg van de SIAD.

**Procedures wederhoor**

De conceptnota van bevindingen hebben wij voorgelegd voor ambtelijk wederhoor aan de SIAD, ter verificatie van het feitenmateriaal. Na verwerking van de reactie van de SIAD, hebben wij de definitieve nota van bevindingen vastgesteld.
Op basis van de definitieve nota van bevindingen hebben wij conclusies en aanbevelingen geformuleerd die, tezamen met de bevindingen, zijn opgenomen in het conceptrapport. Het conceptrapport is voor bestuurlijk wederhoor voorgelegd aan de minister van Financiën. De bestuurlijke reactie van de minister hebben wij, voorzien van een nawoord van de Algemene Rekenkamer, opgenomen in het rapport over dit onderzoek.

# Bijlage 2: Gebruikte afkortingen

| | |
|---|---|
| CAD | Centrale Accountantsdienst |
| DPO | Directie Personeel en Organisatie |
| DRH | Departamento Recurso Humano |
| IT | Informatie Technologie |
| minister van Financiën | Minister van Financiën, Communicatie, Utiliteiten en Energie |
| LMA | Landsverordening Materieel Ambtenarenrecht |
| OM | Openbaar Ministerie |
| P&O | Personeel & Organisatie |
| SIAD | *Servicio di Impuesto, Aduana y Direccion* |
| VDA | Veiligheidsdienst Aruba |

# Bijlage 3: Literatuur

Algemene Rekenkamer (2010). *Stand van zaken integriteitszorg Rijk 2009*. Tweede kamer, vergaderjaar 2009-2010, 32 241, nrs. 1-2. Den Haag: SDU.

Algemene Rekenkamer (2004). *Zorg voor integriteit. Een nulmeting naar integriteitszorg in 2004*. Tweede Kamer, vergaderjaar 2004–2005, 30 087, nrs. 1–2. Den Haag: SDU.

Centrale Accountantsdienst (2010). *Beoordeling van de effectiviteit van het systeem van interne beheersing van de Inspectie der Invoerrechten en Accijnzen*.

Wetenschappelijk Onderzoek- en Documentatiecentrum (2011). *De staat van bestuur van Aruba, Een onderzoek naar de deugdelijkheid van bestuur en de rechtshandhaving*. Meppel: Boom Juridische Uitgevers.

Algemene Rekenkamer

T (297) 582 5448
F (297) 582 7687
E rekenkamer@aruba.gov.aw

Wilhelminastraat 6
Oranjestad
Aruba